ICANN76 | منتدى المجتمع – مناقشة اللجنة الاستشارية الحكومية GAC: انتهاك نظام اسم النطاق DNS
الثلاثاء، 14 مارس/أذار 2023 – من الساعة 10:30 ص إلى الساعة 12:00 م بتوقيت كانكون

جوليا تشارقولين: أهلًا ومرحبًا بكم في مناقشة اللجنة الاستشارية الحكومية GAC في ICANN76 حول انتهاك نظام اسم النطاق DNS يوم الثلاثاء 14 مارس/أذار الساعة 10:30 بالتوقيت المحلي. يُرجى العلم بأن هذه الجلسة يجري تسجيلها وتحكمها معايير السلوك المتوقعة في ICANN.

خلال هذه الجلسة ستقرأ الأسئلة أو التعليقات المقدمة في مربع الدردشة جهرًا إذا كُتبت بالشكل المناسب. إن أردتم التحدث، فيُرجى رفع يدكم من خلال Zoom. ويرجى ذكر الاسم واللغة التي ستتحدث بها في حال كنت ستتحدث بلغة أخرى غير الإنجليزية. ويرجى التحدث بوضوح وبسرعة معقولة للسماح بترجمة دقيقة. ويُرجى التأكد من كتم صوت جميع الأجهزة لديكم الأخرى عند تحدثكم. ويمكنكم الوصول إلى جميع الميزات المتاحة لهذه الجلسة في شريط أدوات Zoom.

وبذلك أسلم الكلمة لرئيسة اللجنة الاستشارية الحكومية GAC. منال إسماعيل تفضلي.

منال إسماعيل: شكرًا جزيلًا يا جوليا. طابت أوقاتكم جميعًا أينما كنتم. مرحبًا بكم من جديد. هذه مناقشة اللجنة الاستشارية الحكومية GAC حول الحدّ من انتهاك نظام اسم النطاق DNS، والمقرر لها مدة ساعة. خلال هذه الجلسة، سنواصل نظر اللجنة الاستشارية الحكومية GAC في مبادرات مؤسسة ICANN ومجتمع ICANN للمنع والحدّ من انتهاك نظام اسم النطاق DNS.

كما سيجري اطلاعنا على التطورات ذات الصلة وسنواصل مناقشة الجهود المحتملة من جانب اللجنة الاستشارية الحكومية GAC للمشاركة مع مجتمع ICANN الأوسع لدعم مراجعات العقود المحسّنة وعمليات وضع السياسات الممكنة للحدّ من انتهاك نظام اسم النطاق DNS على نحو أفضل.

وبدون أي تأخير، اسمحوا لي بتسليم الكلمة إلى قادة الموضوعات. معنا غابرييل أندروز من مكتب التحقيقات الفيدرالي الأمريكي؛ لورين كابين من لجنة التجارة الفيدرالية الأمريكية والرئيس

المشارك لمجموعة عمل السلامة العامة PSWG التابعة للجنة الاستشارية الحكومية GAC؛ كريس لويس-إيفانز من الوكالة الوطنية البريطانية لمكافحة الجريمة والرئيس المشارك لمجموعة عمل السلامة العامة PSWG التابعة للجنة الاستشارية الحكومية GAC. إليك الكلمة يا كريس من فضلك.

كريس لويس-إيفانز: شكرًا جزيلًا يا منال. طابت أوقاتكم أينما كنتم. ننتقل إلى الشريحة التالية من فضلك. سنعقد جلسة حول انتهاك نظام اسم النطاق DNS ولدينا عرض تقديمي من الخارج. ويمكنني رؤية قائد شبكة عمل سياسة الإنترنت والاختصاص القضائي في الزاوية، ونأمل في فرز بعض الشرائح من خلال طاقم الدعم لدينا في اللجنة الاستشارية الحكومية GAC.

سأنطلق بمقدمة سريعة أولًا، قبل ذلك، وأعطي فكرة عن سبب أهمية معالجة انتهاك نظام اسم النطاق DNS. سيكون لدينا بعد ذلك عرض تقديمي حول إحصاءات الجرائم الإلكترونية وكيفية ارتباطها بانتهاك نظام اسم النطاق DNS. ثم سألقي نظرة على الأنشطة الأخرى الجارية داخل المجتمع. ثم سأختتم وسأقدم اعتبارات إما لمشورة البيان الرسمي أو للمسائل ذات الأهمية بالنسبة لنا. ننتقل إلى الشريحة التالية من فضلك. شكرًا.

أشعر غالبًا أنني لا أحتاج إلى تغطية هذه الشريحة. ويبدو أننا نتحدث عن انتهاك نظام اسم النطاق DNS كثيرًا. كانت هناك بعض الجلسات الجيدة بالفعل خلال هذا الاجتماع. سألفت الانتباه مرة أخرى لورشة بناء القدرات يوم السبت. كانت هناك جلسة جيدة لانتهاك نظام اسم النطاق DNS، التي يمكنكم مراجعتها بشأن ذلك.

هنا، لدينا عدد من الروابط التي يمكنكم الانتقال إليها. كما هو الحال دائمًا، يمكنك إجراء بحث داخل موقع ويب اللجنة الاستشارية الحكومية GAC حول انتهاك نظام اسم النطاق DNS وسيظهر عناصر حول البيان الرسمي، وذلك يرجع إلى فريق الدعم. بينيديتا وموظفو الدعم الآخرين حقًا يحدثون ذلك بالمستجدات. إنهم يقومون بعمل جيد حقًا لوجود الموارد التي يمكننا البحث عنها هناك. لدينا عدد من العناصر التي نضع علامات عليها.

وهذا جزء مهم جدًا من عمل مجموعة عمل السلامة العامة PSWG أيضًا. إنه ضمن خطة عملنا، التي صدقنا عليها وصدقنا على هذا الاجتماع، الذي كان جيدًا حقًا، بالنسبة لنا لدعم قدرات مسؤولي إنفاذ القانون والسلامة العامة لحماية الجمهور، وهو ما يفعلونه حقًا في هذا الشأن.

كما قلت، هناك الكثير مما يحدث داخل المجتمع، لذا فهو مهم لأصحاب المصلحة الآخرين داخل المجتمع. هناك الكثير من المناقشات الجارية، ومشاورات مجلس الإدارة والمراسلات. وقد أرسل مجتمع الأعمال عددًا كبيرًا من المعلومات حول مدى أهميته بالنسبة لهم. كانت هناك أيضًا فرق مراجعة – فريق مراجعة المنافسة وثقة المستهلك وخيار المستهلك CCT ومراجعة خدمة دليل التسجيل RDS-WHOIS2 والمراجعة الثانية لأمن واستقرار ومرونة نظام اسم النطاق SSR2 على سبيل المثال لا الحصر – وكذلك عمليات وضع السياسات PDP من المنظمة الداعمة للأسماء العامة GNSO حول الإجراءات القادمة التي تتطرق إلى انتهاك نظام اسم النطاق DNS.

ثم الأخرى، التي سنتطرق إليها لاحقًا في العرض، هي الجهد المبذول من الأطراف المتعاقدة. وقد أرسلوا خطابًا إلى مجلس الإدارة لفتح مفاوضات العقد للمساعدة في معالجة انتهاك نظام اسم النطاق DNS. وهي حقًا خطوة جيدة. فهي تُظهر فقط أن كل فرد في المجتمع يريد اتخاذ إجراء وهو أمر مهم حقًا للجميع، وهذا بالتأكيد سبب نظرنا في الأمر لبعض الوقت.

وبذلك – سألقي نظرة سريعة على فريق الدعم – هل نحن قريبون من –

لورين كابين: لا.

كريس لويس-إيفانز: لا، حسنًا. ربما، غابي، تنبيه هنا.

لورين كابين: هذا هو حيث نتحلى بالمرونة، ونظهر قدرتنا على التكيف مع الظروف الحالية، وأنه يمكننا التمحور.

كريس لويس-إيفانز: نعم. تنبيه يا غابي. أنت التالي. سننتقل إلى عرضنا التقديمي حول اتجاهات الجرائم الإلكترونية. هل يمكننا الانتقال إلى شريحتين، على ما أعتقد، في الحزمة؟ شكرًا. غيب، إليك الكلمة. شكرًا.

غابرييل أندروز: شكرًا. مرحبًا. معكم غابرييل، أتحدث بصفتي هنا كعضو في مجموعة عمل السلامة العامة. وما نأمل أن نفعله هنا هو شيء ربما نشعر بالتفاؤل بأنه يمكننا القيام به على أساس سنوي لاحقًا. لكن السبب في ذلك هو عندما يتعلق الأمر بفهم النطاق والحجم لانتهاك نظام اسم النطاق DNS، مثل محاولة فهم النطاق والحجم لجرائم الإنترنت، فمن المهم أن نعترف بأنه ليس لدينا حقائق كاملة. وما لدينا هو الكثير من وجهات النظر المختلفة.

مثل الأعمى في هذه الصورة الذي قد تتعرف عليه من ورشة بناء القدرات – لقد استخدمتها هناك أيضًا – لدينا الكثير من الأشخاص الذين يبذلون قصارى جهدهم لمراقبة ما هو أمامهم، والتحدث عما يدركونه، على أمل أنه من خلال التعاون، يمكننا الحصول على فكرة أفضل عما هو موجود بالفعل.

إليكم حيث أدرك أن هناك الكثير من جهود المجتمع الكبيرة التي تهدف جميعها إلى توفير البيانات والمقاييس والقياسات والملاحظات حول انتهاك نظام اسم النطاق DNS. وأفكر في أشياء مثل تقارير البوصلة الصادرة عن معهد انتهاك نظام اسم النطاق التي بدأت في خريف العام الماضي. مثل مكتب المدير الفني المسؤول OCTO التابع لمؤسسة ICANN والتبليغ عن نشاط انتهاك النطاق.

سمعت أنه في المحادثة قبل يومين فقط، ربما، مع الموظفين التنفيذيين، ذكر جون كرين أنه بالإضافة إلى ما نتوقعه بالفعل مع التبليغ عن الانتهاك على مستوى أمين السجل، لديه أفكار حول التحليلات المتوقعة والتعلم الآلي الذي يريد أن يدمجه. وأنا متحمس حقًا لمعرفة ما سينتج عن هذه الجهود.

لكن لاستكمال هذه الجهود التي يقودها المجتمع، نأمل في تقديم وجهات نظر أخرى إضافية لا يمكن أن يطرحها على الطاولة سوى إنفاذ القانون والتي تأتي فقط من السلامة العامة. أفكر فيما يتعلق بتبليغ الضحية الذي يأتي إلينا.

لنكن واضحين، لا نقترح أن جميع جرائم الإنترنت هي انتهاك نظام اسم النطاق DNS. بدلًا من ذلك، نفهم أن النطاق والحجم لضرر الضحية الذي يتم إبلاغنا به قد يكون أحد وجهات النظر هذه حيث قد تشعر أنه من المهم مراعاتها في مداولاتك، خاصةً إذا كنا قد نكون مفيدين بطريقة طفيفة للمساعدة لترجمة هذا التبليغ إلى كيف وأين يكون له علاقة بانتهاك نظام اسم النطاق DNS. وبذلك، أعتقد يا كريس، هذا هو الجزء الأول.

كريس لويس-إيفانز: نعم. فقط بإيجاز شديد، قبل أن ننتقل إلى الشريحة التالية. أعتذر. هلا نرجع إلى الشريحة السابقة؟ شكرًا. في آخر اجتماع لنا مع مجموعة عمل السلامة العامة PSWG، وجهنا دعوة إلى جميع الأعضاء لتزويدنا ببعض الإحصائيات التي لديهم عن الجرائم الإلكترونية وكيف يمكن أن يرتبط ذلك بانتهاك نظام اسم النطاق DNS.

في الوقت الحالي، لم نستقبل أي شخص آخر غير الولايات المتحدة والمملكة المتحدة. لذلك إذا كنت تعمل مع وكالات إنفاذ القانون أو وكالات حماية المستهلك عندك، فلا تتردد في منحهم توجيهًا نحونا. سنكون حريصين حقًا على رؤية ما تراه الدول الأخرى وأن نكون قادرين على إجراء مراجعة أوسع لهذه الإحصائيات. ونتطلع إلى القيام بذلك من أجل، ربما على أساس مرة في السنة لإعطائكم فكرة عن المشهد.

بالانتقال إلى شرائح المملكة المتحدة، لدينا في المملكة المتحدة هيئة تبليغ واحدة تسمى Action Fraud، التي لا تتعامل فقط مع الاحتيال. يتعاملون مع الجرائم الإلكترونية كذلك. لكن كان الاسم موجودًا أولًا ثم أضافوا إلى ذلك الاختصاص.

لا تتعقب إحصائيات المجموعة الأربعة الأولى الخاصة بهم حقًا انتهاك نظام اسم النطاق DNS. فلديهم القرصنة ووسائل التواصل الاجتماعي والبريد الإلكتروني. الفيروسات والبرامج الضارة، لذا فإن جانب البرامج الضارة، نوعًا ما، لكن الفيروسات موجودة أيضًا، لذا فهي لا تتوافق حقًا مع ما نفهمه على أنه انتهاك نظام اسم النطاق DNS. ثم القرصنة، سواء أكانت شخصية أم ابتزازًا، التي تميل إلى أن تكون أكثر المواد التي تركز على برمجيات الدفع القسري للفدية. كما ترون من هذه الشريحة، بيانات تعود لعام 2014 واتجاه عام صاعد في التبليغ عن هذه الجرائم. ننتقل إلى الشريحة التالية من فضلك.

أحد الأشياء التي يقومون بها أيضًا هو إجراء استبيانات للشركات والجمعيات الخيرية لفهم مدى تأثرهم، وما يرونه، وكيف يتعاملون مع الأمر. ويدور هذا الجزء من التحليل حول عدد المنظمات التي حددت الانتهاكات أو الهجمات على أنظمتها. ثابت إلى حد ما، ربما يكون هناك اتجاه هبوطي قليلًا على جانب الأعمال. لكن المثير للاهتمام، في الجمعيات الخيرية، ارتفاع واضح.

بعض الأفكار الكامنة وراء ذلك هي الجمعيات الخيرية، قبل القانون العام لحماية البيانات GDPR، ربما لم تكن مهيأة تمامًا للنظر في شبكاتها وإجراء التحليلات. بمجرد أن تبدأ في البحث عن شيء ما، فإنك تميل إلى العثور عليه. لذا، سواء كان هذا أحد أسباب هذه الزيادة، هو أنهم يبحثون عنها ووجدوها، أو كانت زيادة في الهجمات المستهدفة، فمن الصعب جدًا تحديد ذلك. ويمكن أن يكون من الصعب جدًا معرفة ذلك. لكن هناك القليل من الاتجاه في ذلك الشأن. ننتقل إلى الشريحة التالية من فضلك.

في هذه الشريحة، من الواضح، بالنسبة لمن تعرضوا لخرق، تم سؤالهم عن كيفية تحديد هذا الخرق وكيف كان ناقل الهجوم الأولي. على مر السنين، كانت الإجابة عن ذلك، 80% من الوقت، هي التصيّد الاحتيالي. التصيّد الاحتيالي موجود بالتأكيد في مساحة انتهاك نظام اسم النطاق DNS. لذا يمكنكم أن تروا، من كل تلك الجرائم الأخرى لدي في الدفعة الأولى، 80% أو نحو ذلك تتعلق بالتصيّد الاحتيالي، أو أن ناقل الهجوم الأولي كان التصيّد الاحتيالي. لذلك من خلال الحدّ من التصيّد الاحتيالي، يمكن أن يكون لنا تأثير حقيقي على الضرر الناجم عن الجرائم الأخرى التي نتعامل معها على أساس يومي.

ثم يظهر الجزء العلوي الثاني قليلًا مثل التصيّد الاحتيالي. لكن يركز هذا بشكل أكبر على النطاقات المشابهة ورسائل البريد الإلكتروني المُخادعة وهذا الجانب من الأشياء. كان ذلك يمثل أقل بقليل من بقية ذلك. ومن الواضح، بعض أولئك، قد يكون يوجد القليل من التداخل أيضًا. الشريحة التالية من فضلك.

نفس السؤال للجمعيات الخيرية وإجابة مشابهة جدًا. مرة أخرى، 80% تصيّد احتيالي. هناك تحليل قوي حقًا أنه إذا تمكنا من المساعدة في انتهاك نظام اسم النطاق DNS والمساعدة في معالجة التصيّد الاحتيالي، فسيكون لذلك تأثير جيد حقًا على الحدّ من مقدار الجرائم التي تعاني منها هذه الشركات والجمعيات الخيرية. الشريحة التالية من فضلك.

لدينا في المملكة المتحدة خدمة تسمى خدمة التبليغ عن رسائل البريد الإلكتروني المشبوهة. ليست ICANN فقط هي التي تحب الاختصارات. تم إنشاء هذه الخدمة في عام 2020 وهي خدمة يمكن للأفراد أو الشركات من خلالها التبليغ عن رسائل البريد الإلكتروني المشبوهة إلى الحكومة. هذه هي التفاصيل. يقبلون إعادة توجيه البريد الإلكتروني ويقومون أيضًا بإرسال رسائل SMS لأن هذا مصدر كبير آخر لتقارير التصيّد الاحتيالي. وتلقينا 6.4 مليون تقرير في هذه الخدمة، وذلك خلال عام 2022. وذلك حقًا واسع النطاق. الكثير من الضحايا داخل المملكة المتحدة والأشخاص الذين يبلغون عن تلك الرسائل.

كما قلت، تم إطلاقها فقط في عام 2020، ومن الواضح أنها جزء من الاستجابة تجاه بعض الأنشطة التي كانت تجري أثناء الجائحة. لكن منذ ذلك الإطلاق، لدينا 15.8 مليون تقرير في هذه الخدمة. وهو اتجاه تصاعدي لكن لا توجد بيانات كافية في الوقت الحالي لإظهار ذلك. وبالتأكيد، في السنوات القادمة، ربما سأضع ذلك على مخطط بياني صغير لطيف، بلا شك.

بعد ذلك، فيما يتعلق بهذا الأمر بالحكومة، ما يمكن أن يروه من تلك التقارير، من الواضح، أنهم يحاولون التظاهر بأنهم كيان حكومي. لذا في إطار هجمات التصيّد الاحتيالي، كان لديهم إقرارات حول خدماتنا الصحية، وترخيصنا التلفزيوني، وعائداتنا وجماركنا، ثم gov.uk. هناك موقع نطرح فيه جميع معلوماتنا العامة، سواء كانت هذه نصيحة حول ما يجب فعله حيال كوفيد، أو نصائح السفر. كل شيء متوفر هناك. ثم الآخر هو وكالة ترخيص السائقين والمركبات أيضًا. لذلك بالتأكيد الكثير من الهجمات الحكومية وهذه الخدمة كانت مفيدة في القضاء على بعض هؤلاء. الشريحة التالية من فضلك.

لقد تطرقت إلى الأعمال التجارية. من الواضح الآن أن الأفراد ومستخدمي الإنترنت سيتأثرون أيضًا بهذا الأمر وسيبلغوننا عن الجرائم. كانت هناك مراجعة هاتفية لعدد من الضحايا أبلغونا أن نفهم تأثير ذلك عليهم من منظور مالي.

ويمكنكم أن تروا هنا. إنه مخطط بياني مروع. أعتذر. فهذا ما أُعطي لي. لكن يمكنكم أن تروا هنا نطاقًا يتراوح بين 20 و250 جنيه الذي هو على الأرجح الشيء الأكبر الذي يخسره الأشخاص. ولكن عندما تفكرون في ذلك، فهذا ليس بالمال الكثير. لكن بعد ذلك، كان لدينا 6.4 مليون، هذا العام، الأشخاص الذين أبلغوا عن جريمة. وإذا قلت إن كل واحد من هؤلاء فقد حتى 20 جنيهًا، فإن 220 في 6.4 مليون هو عمل يومي جيد أو عمل عام جيد.

لذلك هذا واسع النطاق حقًا عندما تنظرون إليه. وقد يبدو قليلًا. ومع ذلك، من الواضح، خاصةً في هذه اللحظة، مع أزمة تكلفة المعيشة التي نمر بها في عدد من البلدان، فمن المؤثر حقًا أن يخسر الأشخاص هذه الأموال. الشريحة التالية من فضلك.

نتحدث كثيرًا عن المال في الجرائم الإلكترونية. وليس المال فقط هو الذي يؤثر على الأشخاص، خاصةً على الأفراد هنا. تعاني الشركات من فقدان البيانات وهو أمر مؤثر بالنسبة لهم. ولكن على المستوى الفردي، يمكن أن يكون ذلك مؤثرًا حقًا ومزعجًا لهم حقًا.

سأقوم فقط بدراسة حالة سريعة حول هذا الموضوع. تلقينا بعض المعلومات في نظام الشرطة لدينا حول شاب يبلغ من العمر 17 عامًا أفاد بأن أحد المتسللين كان يطلب المزيد من كلمات المرور وكان بإمكانه الوصول إلى عدد من حسابات وسائل التواصل الاجتماعي الخاصة بهم.

كنا قادرين على القيام ببعض الأعمال على خلفية ذلك. وتمكنا من التعرف على المشتبه به، ووجدنا أن لديه سوابق في اختراق حسابات وسائل التواصل الاجتماعي لعدد من الأفراد. وحصلنا على أمر قضائي لزيارة عنوان منزله ووجدنا عددًا من الهواتف النشطة التي كان يستخدمها لارتكاب بعض هذه الجرائم. وعلى تلك الهواتف، كان هناك دليل على التصيّد الاحتيالي الجماعي. ننتقل إلى الشريحة التالية من فضلك.

هذا مثال على أحد الاتصالات. سترون هنا أنه يمثل شخصًا ما وجد بعض المعلومات عن فرد ما ويقول: "لقد عثرت على بعض الصور لك على أحد المواقع. وقد ترغب في فعل شيء حيال ذلك." يعود الشخص ويقول: "ما الرابط؟" ثم ينشر هذا الشخص رابطًا لينتقلوا إليه.

وعند مراجعة الهواتف، وجدنا مئات الرسائل المرسلة إلى الفتيات الصغيرات، بشكل عام، في محاولة للوصول إلى حساباتهن. لذلك ترون هنا، من نطاق واحد أو فرد واحد، قد يكون لديه مئات الضحايا. إنه ليس شيئًا موازيًا، نطاق واحد، ضحية واحدة. يمكن أن يكون نطاقًا واحدًا، مئات الضحايا. ويتوقف كل هذا على نوع الهجوم وطريقة استخدامه في كيفية عمل ذلك. لقد بحثنا أيضًا في ذلك الموقع، بوضوح، لنرى كيف كان هذا الشخص يستخدم ذلك لابتزاز الآخرين. ننتقل إلى الشريحة التالية من فضلك.

ستكون هذه الشريحة معقدة بعض الشيء، لذا أعتذر مقدمًا، وصغيرة بعض الشيء، لكنها صغيرة لسبب ما. أعلى يمين الشاشة توجد خدمة تصيّد احتيالي مستضافة على الإنترنت تمنح المستخدمين المسجلين القدرة على شراء صفحات تصيّد احتيالي والحصول عليها على الإنترنت. تقوم بالنقر

فوق إحداها، سواء كانت Netflix أو Facebook أو Snapchat أو أي من الأشياء الأخرى. ويمكنك حتى اختيار اللغة التي تريدها. صغيرة جدًا هنا ولكن هناك الإنجليزية والإسبانية والفرنسية والروسية، على ما أعتقد، كل ذلك هناك. ويمكنك تحديد اللغات التي تريد الظهور عليها. وتدفع مقابل هذه الخدمة.

ثم، أسفل اليسار، يوجد مثال على Snapchat. سيتم إنشاء نطاق ضار يمكنك بعد ذلك إرفاقه برسالتك. سيؤدي ذلك بعد ذلك إلى حصاد التفاصيل نيابةً عنك. الصورة السفلية هي مثال على لوحة التحكم التي قاموا بإنشائها، التي يمكنك بعد ذلك الانتقال إلها والاطلاع على جميع بيانات الاعتماد التي تم حصادها.

من الواضح، بمجرد حصاد بيانات الاعتماد، هذا هو المكان الذي يبدؤون فيه بالابتزاز. يلتقطون الصور المخزنة هناك، سواء كانت خاصة، أو كان Google Drive، أو حتى لم تتم مشاركتها على وسائل التواصل الاجتماعي. وهذا له تأثير حقيقي كبير على الأشخاص.

تمكنا من إزالة هذا الموقع بدعم من أمناء السجلات. ونشكرهم على ذلك. ويمثل الشخص المتورط أمام المحكمة الشهر المقبل، ولكن في الوقت الحالي، هو محبوس احتياطيًا بسبب التهديد الذي يمثله على عدد الضحايا. وفي ذلك، الأمر المهم حقًا.

من الواضح أننا حاولنا الاتصال بكل ضحية تمكنا من تحديدها وتمكنا من إبلاغهم بأننا قمنا بتأمين بياناتهم، وقمنا بإزالتها، ونقترح عليهم تحديث كلمات المرور الخاصة بهم وكل شيء آخر. من المهم حقًا فهم هذا التأثير بالنسبة لهم. وتلقينا الكثير: "أوه، شكرًا لكم على القيام بذلك. لم أكن أعرف كيف أتصدى له." وحقًا إنه أمر أساسي هنا حول كيفية معالجتنا للأمر وكيفية أزالتنا لبعض هذا الضرر الذي حدث.

ننتقل إلى الشريحة التالية. أعتقد أنني سأسلم الكلمة إلى غابي.

لورين كابين: أتساءل فيما يتعلق بالعرض التقديمي لزميلنا برتراند. هل أنت مستعد للانطلاق؟ هل تفضل الانطلاق الآن أم تفضل... ما رأيك؟

كريس لويس-إيفانز: أعتقد أننا سنقوم بعمل غابي لأنه يسير بشكل جيد. ثم سنعود. أعتذر. لدي شريحة أخرى. هذا مجرد ملخص لبيانات الأعمال والأفراد معًا. أحدث تقرير كان من عام 2020 إلى عام 2021. داخل المملكة المتحدة، تلقوا 875000 تقرير عن الاحتيال والجرائم الإلكترونية. أعتذر. يجب أن يتم الجمع بينهما. ويبلغ ذلك عن خسائر بقيمة 2.35 مليار في ذلك التقرير.

ثم نسبة 80% من هذا الاحتيال كانت تعمل عبر الإنترنت أيضًا، سواء كان ذلك من بريد إلكتروني للتصيّد الاحتيالي أو غير ذلك. لذا فإن قدرًا كبيرًا من هذه الخسارة يعود إلى شكل من أشكال النشاط الذي يعمل عبر الإنترنت. وكما قلنا من قبل، رسائل التصيّد الاحتيالي عبر البريد الإلكتروني، ربما يكون 80% منها، عامل تمكين كبير حقًا للمجرمين لاستخدامه في شن هجماتهم الإلكترونية. وهذه بالتأكيد آخر شريحة قبل أن أنتقل إلى غابي.

غابرييل أندروز: هل يمكننا الانتقال للشريحة التالية؟ شكرًا. من منظور الولايات المتحدة. ومرة أخرى، كما قال كريس، نأمل حقًا أن يكون هناك أشخاص آخرون يمكنهم تشجيع وكالات إنفاذ القانون على مشاركة وجهات النظر من جميع أنحاء العالم.

أصدر مكتب التحقيقات الفيدرالي FBI بالفعل، الأسبوع الماضي، تقرير جرائم الإنترنت الخاص به لعام 2022، وأصبح هذا الأمر رائجًا في الصحافة. وهذا هو السبب أيضًا في أنني أعتقد أن القدرة على التحدث عن هذا على أساس سنوي أمر جيد لأننا نحب أن نكون قادرين على مشاركة هذه المعلومات عندما تصدر وتكون حديثة.

هذه البيانات هي ملخص لجميع شكاوى الضحايا التي ترد إلى مركز شكاوى جرائم الإنترنت. وهي البوابة المركزية التي نتلقى من خلالها كل هذه الأرقام ونجمعها. ثم يعودون ثم ينشرون تقارير مبنية على ذلك. لكن تجدر الإشارة إلى أن هذه ليست صورة لكل جرائم الإنترنت الموجودة. إنها فقط ما يتم إبلاغنا به. الشريحة التالية من فضلك.

على مدى السنوات الخمس الماضية، تلقى IC3 – مرة أخرى، هذا هو اختصار مركز شكاوى جرائم الإنترنت – ما معدله 650 ألف شكوى سنويًا. ويصل هذا إلى ما يزيد قليلًا عن 2000 شكوى يوميًا، لذا فهو رقم معقول. لكنه لا يزال أقل بكثير من تمثيل المقدار الحقيقي للجريمة الموجودة. ونعلم أننا لا نتلقى جميع الشكاوى طوال الوقت.

الشيء الوحيد المثير للاهتمام لملاحظته هنا هو أنه عندما تنظرون إلى عدد الشكاوى الفعلية – الأشخاص الذين يصلون إلينا – ظلت مستقرة نسبيًا خلال السنوات الثلاث الماضية، وهو أمر مثير للاهتمام. لكن حجم الخسائر زاد بشكل مطرد. وأتمنى لو كان لدي تفسير جيد لكم عن سبب ذلك. ليس لدينا تفسير رائع حقًا لذلك في هذا الوقت، لكن من المؤكد أنه شيء مثير للاهتمام لنلاحظه. ويوضح أن الضرر مستمر، حتى إذا ظل العدد النسبي للشكاوى مستقرًا. يُرجى المتابعة إلى الشريحة التالية.

كما ذكر كريس ضمن فئات الجرائم الخاصة بهم وكيف قاموا بتجميعها، فإننا لا نتتبع انتهاك نظام اسم النطاق DNS كفئة أيضًا. ولكن هناك فئات لانتهاك نظام اسم النطاق DNS يتم تتبعها في تقارير مركز شكاوى جرائم الإنترنت IC3 الخاصة بنا. وأشير هنا على وجه الخصوص، في الأسفل، إلى التصيّد الاحتيالي. عندما ننظر إلى الفئات الخمس الأولى لجرائم الإنترنت التي تم تبليغها إلينا، نرى أن التصيّد الاحتيالي هو الفئة الأولى.

علاوة على ذلك، نظرًا لأن هذا يظهر خلال السنوات الخمس الماضية، يمكنكم أن تروا أنه لسبب أو لآخر، ارتفع التصيّد الاحتيالي بشكل كبير من خمس سنوات مضت إلى ما هو عليه اليوم، على الأقل من حيث الشكاوى التي نتلقاها. الشريحة التالية.

وهذا، مرة أخرى، يعرض فقط جميع فئات الجريمة، وليس فقط أعلى خمسة، ويظهر مدى ارتباط التصيّد الاحتيالي بها. هناك شيء يجب تسليط الضوء عليه هنا، كما ذكر كريس بالفعل، هو أن التصيّد الاحتيالي، بينما يتم تعقبه كفئة لديهم، غالبًا ما يكون الطريقة الأولية التي يستخدمها الأشرار لاختراق الضحايا لعدد من فئات الجرائم الأخرى الموجودة هنا أيضًا.

فقط كمثال، قد تسأل، "هل تعد برمجيات الدفع القسري للفدية انتهاكًا لنظام اسم النطاق DNS؟" لا. ليست كذلك. برمجيات الدفع القسري للفدية هي عندما يأخذ أحد الأشرار بياناتك من على جهازك، ويقومون بتشفيرها، ولا يسمحون لك بالحصول عليها إلا إذا دفعت لهم فدية. ولكن إذا طرحت السؤال: "هل تنتشر برمجيات الدفع القسري للفدية عن طريق التصيّد الاحتيالي؟" فالجواب على ذلك هو نعم.

هناك تقرير صدر الأسبوع الماضي من CISA، إحدى الوكالات الشقيقة، حول نوع جديد من برامج الفدية يسمى برمجيات الدفع القسري للفدية الملكية Royal ransomware. في هذا

التقرير، قدروا أن 67% من إصابات برمجيات الدفع القسري للفدية الملكية جاءت من التصيّد الاحتيالي. مرة أخرى، نتتبع الفئة الأولية في ذلك الشأن ولكن لها تأثير تالي.

وبالتالي، فقط لتوضيح هذه النقطة، عندما يتخذ أصدقاؤنا والمتعاونون والزملاء في مجتمع ICANN الموجودون على مستوى أمين السجل أو السجل إجراء مسؤول لمكافحة الانتهاك لمعالجة النطاقات المسجلة بقصد تسبيب الضرر المستخدمة في التصيّد الاحتيالي، فإنهم يساعدون ليس فقط في معالجة النوع الأكثر شيوعًا من جرائم الإنترنت التي تأتي إلينا ولكن أيضًا جميع الفئات الأخرى التي تم تمكينها من خلال ذلك. الشريحة التالية.

بالإضافة إلى مشاركة هذه الإحصائيات من التقرير السنوي، سألت عددًا من زملائي أيضًا: "مرحبًا، ما الجديد الجاري؟ ما الجديد، والقادم، والمبتكر للاتجاهات؟ ما هو الجدير بالملاحظة في الأشهر الأخيرة؟" وما عادوا إليّ به كان شيئًا يسمونه "الإعلانات الخبيثة." ولصالح المترجمين، يعد هذا مزيجًا من البرامج الضارة والإعلانات معًا. لقد حظي ذلك بالكثير من الاهتمام، بدءًا من شهر ديسمبر/كانون الأول تقريبًا من العام الماضي وحتى الأشهر القليلة الأولى من هذا العام.

كما هو الحال في التصيّد الاحتيالي، يحصل أحد الأشرار هنا على اسم نطاق مشابه تم تسجيله لأغراض مخالفة. وفي بعض الأحيان، يحصلون على اسم نطاق قد يبدو كحزمة برامج، أو علامة تجارية أخرى موثوقة، أو خدمة ما. لكن بدلًا من استخدام ذلك في البريد الإلكتروني، بدلًا من ذلك، ينتقلون إلى موفري محرك البحث ويشترون الإعلانات.

في هذه الحالة التي تراها على الشاشة هنا، المصدر Abuse CH. لقد أخذته من موجز Twitter الخاص بهم. يتظاهر الشرير في هذه الحالة بأنه يمتلك موقعًا مرتبطًا بعميل بريد Thunderbird الشرعي. ونوع من البرامج يحبها الكثير من الأشخاص. لكن من الواضح أنهم لا يشاركونها فقط من منطلق طيبة القلب.

إذا انتقلت إلى موقعه الإعلاني في الجزء العلوي، فستحصل على هذا البرنامج بالإضافة إلى البرامج الضارة على جهازك – في هذه الحالة، IcedID. وهو شكل من أشكال حصان طروادة المصرفي. إذا تم تثبيته على جهازك، فسيلتقط في النهاية عند تسجيل الدخول إلى البنك الذي تتعامل معه، ويسرق بيانات اعتماد تسجيل الدخول، ثم يحاول استنزاف الحسابات.

لذا فإن هذا الاتجاه الجديد مثير للاهتمام لأنه لا يزال يعتمد على تلك النطاقات المسجلة بقصد تسبيب الضرر. هل هذا تصيّد احتيالي في حد ذاته؟ ربما لا، لأنه لا يوجد اتصال بريد إلكتروني في هذا الأمر. لكن لا يزال له نفس النتيجة النهائية. وأذكر هذا، أولًا، لأنه جديد؛ ثانيًا، لأنه يحتوي على علاقة مباشرة بنظام اسم النطاق DNS؛ لكن ثالثًا، لأنني أعتقد أيضًا أنه من المهم أن ندرك أنه يجب أن نتحلى بالمرونة والذكاء في الاستجابة للمواقف العالم الحقيقي وأن نكون مستعدين لدمج هذه الاتجاهات الجديدة في أفكارنا حول ما يمكننا معالجته.

ولكن كما كان من قبل، فإن أمناء السجلات المسؤولين الذين يتخذون إجراءات ضد النطاقات المسجلة بقصد تسبيب الضرر يعالجون هذا أيضًا، وهذا أمر جيد. الشريحة التالية. وستكون هذه شريحتي الأخيرة.

أريد فقط أن أتعمق في هذه النقطة. في اللغة الإنجليزية، نقول هنا "النفخ في قربة مثقوبة". لكن التصيّد الاحتيالي مقبول بشكل عام بين جميع أعضاء مجتمعنا هنا داخل ICANN باعتباره انتهاكًا لنظام اسم النطاق DNS. وهو أيضًا، كما علمت للتو من أحدث تقاريرنا، هو حاليًا أكثر أنواع جرائم الإنترنت التي يتم التبليغ عنها. ويتيح التصيّد الاحتيالي ارتكاب العديد من الجرائم الأخرى.

من المهم اتخاذ إجراء سريع ضد النطاقات المسجلة بقصد تسبيب الضرر والتحفيز الذي يمكننا تقديمه من خلال سياساتنا هنا. فهو يؤثر على ما نراه. كانت هذه الحقائق الرئيسية لدي وأقدر اهتمامكم.

أعتقد الآن أن برتراند بجانبي ومستعد، يمكننا الانتقال إليه.

منال إسماعيل: نعم، من فضلك يا برتراند. تفضل. وشكرًا جزيلًا لشبكة عمل سياسة الإنترنت والاختصاص القضائي على التواصل دائمًا مع اللجنة الاستشارية الحكومية GAC واطلاعنا على العمل الذي تقومون به فيما يتعلق بانتهاك نظام اسم النطاق DNS، الذي من الواضح أنه موضوع ذو أهمية كبيرة للجنة الاستشارية الحكومية GAC. شكرًا.

برتراند دو لا تشابيل: شكرًا جزيلًا يا منال. يسعدني أن أعود إلى اللجنة الاستشارية الحكومية GAC لأنني اعتدت أن أكون هنا كممثل لفرنسا منذ سنوات عديدة، وأيضًا بصفتي نائب رئيس اللجنة الاستشارية الحكومية GAC. وأرى بعض الوجوه المألوفة من تلك الأيام. ويسعدني أن تتاح لي الفرصة للتقديم هنا.

أنا المدير التنفيذي لشبكة عمل سياسة الإنترنت والاختصاص القضائي، وهي منظمة شاركت في تأسيسها منذ 10 سنوات حتى الآن. ويسعدني جدًا الحضور إلى هنا والتحدث عن هذا النقاش الذي حرك مجتمع ICANN لعدة سنوات والإشارة قليلًا إلى ما كنا نعمل عليه للمساعدة في المضي قدمًا في النقاش والمضي قدمًا نحو الحلول.

شبكة عمل سياسة الإنترنت والاختصاص القضائي هي... أجيث فرانسيس، الموجود في الخلف هنا، هو مدير البرامج هناك. نحن مبادرة أصحاب مصلحة متعددين، حيث نجمع بين الحكومات والشركات والمشغلين الفنيين والأوساط الأكاديمية والمجتمع المدني والمنظمات الدولية للتعامل مع تحديات الاختصاص القضائي على الإنترنت.

لدينا على وجه الخصوص – الشريحة التالية من فضلك – ثلاثة برامج ولن أتحدث عن البرنامجين الأولين بالتفصيل. لكن أحدها مخصص تحت التسمية النطاقات والاختصاص القضائي، لمسألة على وجه التحديد متى يكون من المناسب التصرف على مستوى نظام اسم النطاق DNS لمعالجة الانتهاكات؟ وهناك مجموعة اتصال تعمل منذ أكثر من خمس سنوات حتى الآن مع حوالي 40 شخصًا من مجتمعات مختلفة.

يسعدني جدًا أن أقول إن منال كانت كريمة جدًا، وأن أشخاصًا آخرين هنا، بمن فيهم سوزان، شاركوا بنشاط في العمل. وأنا ممتن لها بشكل خاص، بالنظر إلى العبء الثقيل الذي تتحمله، لأنها صرفت وقتًا للمشاركة. وكان من مهمًا.

بشكل أساسي – الشريحة التالية من فضلك – المهم هو ما نتحدث عنه هنا، كيف نكافح الانتهاكات الموجودة على الإنترنت؟ هذه الانتهاكات متنوعة للغاية. يظهر العرض الذي أمامي أن براعة الإنسان بلا حدود على الإطلاق. كل طريقة يمكننا من خلالها انتهاك شيء ما سيتم انتهاكها. وكلنا نعرف ذلك.

لذا فإن التحدي الرئيسي هو أنه في معظم الحالات – وهذه هي النقطة الثانية – هذه مشكلة عابرة للحدود الوطنية. ومن المثير للاهتمام بصورة خاصة التحدث عن هذا في اللجنة الاستشارية الحكومية GAC لأنكم ممثلون لحكومات. ولقد كنت ممثلًا لحكومة. ونعلم جميعًا أن سبب وجود مشكلة في معالجة الانتهاكات عبر الإنترنت هو أننا لا نملك أدوات التعاون بين الحكومات للعمل عبر الحدود الوطنية. فلدينا هيكل دولي يقوم على الفصل بين السيادات والتعاون صعب للغاية.

أحد البرامج التي لدينا هو معالجة الوصول عبر الحدود إلى الأدلة الإلكترونية. وهي قضية إشكالية للغاية وتستغرق سنوات لتنظيم الإجراءات القانونية الواجبة بين الدول لإجراء التحقيقات باستخدام الأدلة الإلكترونية. فالمشكلة التي نتصدى لها هي أنه ليست فقط الشبكة عالمية، وليس فقط أن الفاعلين يعملون بحرية عبر الحدود، لكن الأدوات التي لدينا للتعامل مع ذلك ليست فعالة وليست موجودة لتسهيل التعاون الحكومي الدولي.

الشيء التالي هو أنه من أجل معالجة هذه المشاكل، هناك حاجة إلى فهم أفضل لكيفية عمل الإنترنت نفسه. عندما نتحدث عن نظام اسم النطاق DNS، هناك نقص في الفهم لدى العديد من الدوائر، الأمر الذي ربما تكونون على دراية به عندما تتحدث مع الزملاء، حول كيفية عمل هذه البنية. إذا كنتم ترغبون في فهم كيفية الوصول إلى المسجَّل، ومعرفة كيفية عمل نظام WHOIS، فستجدون المسجَّل وما إلى ذلك. هذا ليس بالأمر السهل للغاية.

الشيء التالي، والأكثر أهمية، هو أنني كنت أتحدث عن نقص الأدوات ولكن هناك أيضًا مسألة الاختصاصات. يقوم مشغلو نظام اسم النطاق DNS بشكل أساسي بتوفير أسماء النطاقات. ليس لديهم أي اختصاص، بشكل أساسي، في فحص ما إذا كان تصيّدًا، ما إذا كان برنامجًا ضارًا، لذلك يعتمدون على المُخطِرين. بل إن الأمر الأسوأ – سأعود إلى ذلك لاحقًا – عندما نتحدث عن الانتهاكات المتعلقة بالمحتوى. كيف يمكنك تقييم شرعية محتوى لخليط من الاختصاصات القضائية.

أذكر الموارد لأن التحقيق في أي حالات فردية – ويمكن أن تصل إلى مئات الآلاف – يستغرق وقتًا. هذه صناعة بطيئة نسبيًا وصغيرة الهامش.

خلاصة القول هي أن هذه مشكلة تمثل مشكلة للجميع. ومشكلة للحكومات لأنكم تشعرون بالقلق، بصورة مشروعة، من عدم معالجة الانتهاكات. ومشكلة للشركات لأنها أيضًا ضحايا أو لديها عبء في معالجة هذه الأمور. ومشكلة للمستخدمين.

لذا فالشيء التالي هو أننا بحاجة إلى فهم – الشريحة التالية من فضلك – شيء أساسي. تعلمون بهذا ولكني أريد مشاركة ما أشاركه بصورة متكررة مع أشخاص خارج بيئتنا لأنهم لا يعرفون بالضرورة كيف يعمل النظام بالضبط. وبالتالي العلاقة بين المسجِّل وأمناء السجلات والسجلات والمستخدمين؛ الاستعلامات التي تنتقل من واحد إلى آخر؛ والأدوار التي تلعبها الجهات الفاعلة المختلفة في جعل الإنترنت الذي نعرفه يعمل بالطريقة التي نريده أن يعمل بها.

هذه بنية لن أتطرق إليها. النقطة التي أريد توضيحها هي أنه لا يوجد سوى أربعة إجراءات يمكن لمشغلي نظام اسم النطاق DNS اتخاذها فيما يتعلق بأسماء النطاقات.

الأول – الشريحة التالية، من فضلك – هو أنه يمكنكم قفل النطاق. في الأساس، لا يمكنكم تغيير المعلومات التي قدمها المسجِّل. ولا يمكنكم إجراء النقل أو الحذف أو التعديل. ولا يمكنكم تغيير الخادم أو عنوان بروتوكول الإنترنت IP الذي تم ذكره. الأهم من ذلك، أن هذا الإجراء لا يجعل المحتوى غير قابل للوصول. إنما جزئيًا يمكنك قفله. وهذا جيد للتحقيق بعد ذلك. لكنه لا يغير أي شيء فيما يتعلق بالوظائف.

العنصر الثاني هو أنه يمكنكم تعليقه. في هذا الصدد، تأخذ اسم النطاق، وتحذفه من ملف منطقة نطاق المستوى الأعلى TLD العام، ولا يتم حل النطاق. لا يمكنكم تغيير المعلومات، أيضًا، فيما يتعلق بالخادم. لكن هنا، مرة أخرى، لا يزال النظام يعمل. إذا كنتم تستخدمون عنوان بروتوكول إنترنت IP، فلا يزال بإمكانكم الوصول إلى العنصر.

العنصر الثالث هو إعادة التوجيه. غالبًا ما يستخدم هذا الإجراء لتغيير مجرى اسم نطاق معين عندما تريدون إجراء تحقيق. إنه في الأساس يعدل ملف المنطقة لإعادة التوجيه إلى خادم آخر لمراقبة السلوك وتحديد الضحايا وأشياء من هذا القبيل.

العنصر الرابع هو النقل، عندما تضع النطاق لدى أمين سجل آخر. يمكن أن يحدث هذا عندما يتم التسجيل بطريقة خاطئة لدى أمين سجل معين. ولكن لأي سبب من الأسباب، هناك مصلحة في وضعه، على سبيل المثال، لدى أمين سجل الملاذ الأخير، وهو أمر يشارك فيه بينيديكت أديس بنشاط كبير.

الشريحة التالية مهمة لأن هذه هي الإجراءات الأربعة. يمكنك الحذف ولكني لا أفكر في الحذف لأنه ليس إجراءً موصى به لأسباب مختلفة. السؤال الرئيسي هو: هل التصرف على مستوى

نظام اسم النطاق DNS، بهذه الإجراءات الأربعة فقط، هو الأداة الصحيحة للتعامل مع الانتهاكات؟

الجواب نعم في حالات معينة ولا في حالات أخرى. وليس الدواء الشامل المثالي. وليس بالأساس ما يميل بعض الأشخاص خارج مجتمعاتنا إلى اعتباره نوعًا ما لوحة تحكم كبيرة. كما لو كانت لديك مشكلة في اسم نطاق أو مرتبطة باسم نطاق، ما عليك سوى قلب المفتاح وستختفي المشكلة. ليس هذا هو الحال ولكن من المفيد أن يكون لديك إجراءات في حالات معينة.

لذا فإن المشاكل الرئيسية، أو المسائل الرئيسية، هي التالية. أولًا، إنها أداة لا تعالج فقط خدمة الوصول إلى موقع اسم النطاق ولكن أيضًا الكثير من الخدمات الإضافية. يمكن أن يكون ذلك رسائل بريد إلكتروني، ونقل ملفات، وأشياء أخرى. لذا فهي أداة غير حادة للغاية.

الشيء الثاني هو أن لها تأثير عالمي. فهي تغطي العالم كله. ليست دقيقة. لا تحظرون جغرافيًا تعليق اسم نطاق. هنا، الأمر مثير للاهتمام لأنه يمكنكم رؤية ذلك كميزة أو خطأ. باعتبارها خطأ، فلها تأثير عالمي لذا فهي ليست دقيقة. ولكن عند الربط بما كنت أقوله من قبل، فإننا نفتقر إلى أدوات التعاون الدولي. إن امتلاك شيء له تأثير عالمي مفيد في حالات معينة.

الشيء التالي، كما قلت، لا يزال بإمكانكم الوصول إلى معظم الخدمات من خلال عنوان بروتوكول الإنترنت IP. بعد ذلك، أنتم في موقف يكون فيه مشغلو نظام اسم النطاق DNS جزءًا من منظومة أكبر. نحتاج إلى أن نأخذ في الاعتبار البنية العام، بما في ذلك موفري الاستضافة وموفري خدمات الإنترنت والجهات الفاعلة الأخرى التي يمكن أن يكون لها إجراءات أيضًا. المهم هو العمل على المستوى الصحيح.

النقطة التالية، حاليًا، في اتفاقيات اعتماد أمين السجل والسجل مع ICANN، هناك التزام بوجود نقاط انتهاك والتحقيق فيها، لكن هناك عددًا محدودًا من الالتزامات التي توضح ما هو مطلوب حقًا وما هو ضروري حقًا.

يؤدي هذا إلى الموقف الذي شهدناه لفترة طويلة من الزمن، الذي كان ولا يزال نقاشًا مطولًا داخل ICANN، لسنوات عديدة، حول كلمة "انتهاك نظام اسم النطاق DNS" وتحديد ما تعنيه. وكان للأشخاص مواقف مختلفة للغاية في هذا الصدد. جلسات كثيرة لعدة سنوات حول ذلك الأمر. ونقد بين مختلف الدوائر حول ما إذا كان التعريف هو هذا التعريف أم ذاك. وحتى التوترات داخل الدوائر المختلفة فيما يتعلق بحجم الإجراءات التي ينبغي اتخاذها أم لا.

لا يعني ذلك أنها جهات فاعلة سيئة. نعلم أنه توجد جهات فاعلة سيئة. توجد جهات فاعلة أكثر مسؤولية من غيرها. لكن من الواضح أنه لا توجد طريقة للتحرك نحو توافق في الآراء في ذلك الأمر. وكانت النتيجة هذا الشعور بالإحباط.

خلاصة القول هي أنكم إذا طرحتم سؤالًا خاطئًا، فمن غير المرجح أن تحصلوا على الإجابة الصحيحة، الأمر الذي يتطلب إعادة صياغة للمشكلة. إعادة الصياغة، إلى الشريحة التالية، هل السؤال الحقيقي هو: متى يكون من المناسب التصرف على مستوى نظام اسم النطاق DNS لمعالجة الانتهاكات عبر الإنترنت؟ أعتقد أن هذه صياغة يمكن أن يتفق عليها الجميع باعتبارها صيغة صحيحة تأخذ في الاعتبار العناصر المختلفة.

الشريحة التالية... كجزء من إعادة الصياغة هذه، كنا نعمل مع مجموعة الاتصال التي ذكرتها سابقًا لفترة طويلة من الوقت وقمنا بتضييق نطاق فهم انتهاك نظام اسم النطاق DNS، الذي أطلقنا عليه في وقت ما الانتهاك الفني. ولكن بمساعدة بعض الجهات الفاعلة، قمنا بتضييق فكرة أن انتهاك نظام اسم النطاق DNS يجب اعتباره أنه تلك الأشياء الخمسة: تداول البرامج الضارة، والروبوتات، والتصيّد الاحتيالي، وهجمة تزوير المواقع الإلكترونية، والبريد العشوائي إلى الحد الذي يتم استخدامه كآلية انتشار لما سبق.

يمكنكم العثور على مزيد من التفاصيل حول تعريفات هذه الأشياء الخمسة، أولًا في المناهج التشغيلية التي أصدرتها شبكة سياسة الإنترنت والاختصاص القضائي I&JPN في أبريل/نيسان 2019. أدى ذلك إلى دمج هذه التعريفات الخاصة بانتهاك نظام اسم النطاق DNS في إطار عمل معالجة الانتهاكات الذي أصدره عدد معين من الجهات الفاعلة داخل المجتمع في ديسمبر/كانون الأول 2019، وفيما بعد، تقرير اللجنة الاستشارية للأمن والاستقرار SSAC 115 في عام 2021 الذي أدرج هذا التعريف لانتهاك نظام اسم النطاق DNS.

قد لا يكون هذا هو التعريف المثالي ولكنه عنصر مهم للغاية للتمييز بين هذا، ذلك الذي يمكننا أن نطلق عليه انتهاك نظام اسم النطاق DNS، وأن كل جهة فاعلة تفهمه لديها سبب للتحقيق ويقع ضمن اختصاص المشغلين، من الانتهاك التي يرتبط بالمحتوى الذي سأتناوله لاحقًا.

في هذا السياق، قمنا بإصدار – ولن أخوض في جميع التفاصيل – مجموعة أدوات في عام 2021 أشجعكم على الانتقال إليها ومشاهدتها عبر الإنترنت لمساعدة مشغلي نظام اسم النطاق

DNS والمُخطِرين والمشرعين أو سلطات إنفاذ القانون على فهم المتغيرات المختلفة والعناصر الإرشادية للتقارب والعمل معًا.

تذكر الشريحة التالية عنصرًا مهمًا وهو أن هناك سير عمل حول أربعة عناصر في التعامل مع أي نوع من الانتهاك. الأول هو في الأساس تحديد الانتهاك نفسه. يمكن أن يكون من المُخطِرين أو من المشغلين أنفسهم. والثاني هو تقييم هذا الانتهاك. هل هو بالفعل ما يبرر اتخاذ إجراء على مستوى نظام اسم النطاق DNS؟

والثالث ما هو الإجراء الذي ينبغي اتخاذه بين الأربعة الذين ذكرتهم؟ والخامس هو شيء لم نناقشه بعد ولكنه جزء من المشهد، وهو سبل اللجوء عندما يكون هناك قرار تم اتخاذه ويجب تغييره، لأي سبب كان. ويمكن أن تحدث الأخطاء.

بدون التفصيل كثيرًا، في كل مرحلة من هذه المراحل، أنتجنا عددًا معينًا من الأشياء، مثل تحديد أنواع الانتهاكات بشكل أكثر وضوحًا. الإشارة إلى العناصر المتعلقة بما ينبغي أن يفعله المُخطِرون، من حيث العناية اللازمة، لتوثيق تلك العناصر. ولا يكفي مجرد إرسال إشعار بدون أي دليل مستدام عليه. ما هي شروط إخطار المسجَّل، خاصةً عندما يتم اختراق المواقع؟

عند التقييم، هناك سؤال أساسي حول ما هي العتبات ومعايير الإجراء؟ متى يكون من الضروري تلبية عتبة ما؟ واختيار الإجراء. هناك أنواع مختلفة من الإجراءات، كما ذكرت. وهناك وثيقة تشرح بدقة الرسومات التي عرضتها عليكم من قبل. وأخيرًا، فيما يتعلق باللجوء، هناك مسألة قنوات اللجوء والعناصر المتعلقة بالشفافية.

هذه عملية. وكل ما يرتبط بالتحقيقات في محاولة معالجة الانتهاكات يمر بمراحل مختلفة تتضمن التعاون بين مختلف الجهات الفاعلة. إذا انتقلتم إلى الشريحة التالية، في هذا السياق، يكون فريق الاتصال قد أنتج سلسلة من الوثائق التي آمل أن تكون مفيدة لكم كمجتمع لكنها مفيدة في المناقشة العامة.

السؤال الأول يتعلق بما يجب أن تحتويه الإشعارات؟ ما هي مكونات الإشعارات التي تدعم الأدلة؟ والثاني ما هي أنواع المُخطِرين؟ هل نفس الشيء أن تكون مُخطِرًا لصور الاعتداء الجنسي على الأطفال أو لانتهاك العلامات التجارية، على سبيل المثال؟

والشيء التالي، كما قلت، ما هي العناية اللازمة التي يجب على المُخطِرين القيام بها للتأكد من أن عبء التحقق لا يقع بالكامل على المشغلين؟ ما هو نوع الترتيب الذي يمكن إجراؤه بين المُخطِرين الموثوق بهم؟ ما هو الترتيب للمُخطِرين الموثوق بهم؟

أريد أن أوضح ذلك. لا أحد يستطيع أن يقول بمفرده: "أنا مُخطِر موثوق به." في أحسن الأحوال، يمكنك أن تقول: "لدي خبرة في هذا المجال بالذات تجعلني مُخطرًا خبيرًا." فعلاقة المُخطِر الموثوق به هي اعتراف ثنائي الجانب. يمكنك أن تكون مُخطِرًا موثوقًا به لمشغل واحد ولكن ليس للآخرين. فهو تمييز مهم ونحتاج إلى مزيد من العمل على فكرة المُخطِرين.

هناك وثيقة مخصصة تتناول مسألة الروبوتات. وليس لدي وقت للدخول في التفاصيل. لكن هناك قضية مهمة للغاية تسمى النطاقات التي يتم إنشاؤها بواسطة الخوارزميات. ويعد العثور على تعاون أفضل بين إنفاذ القانون وICANN ومشغلي نظام اسم النطاق DNS حول النطاقات التي يتم إنشاؤها بواسطة الخوارزميات عنصرًا مهمًا للغاية. أعتقد أن هذه الوثيقة ساعدت في دفع المناقشة إلى الأمام قليلًا.

وأخيرًا، فيما يتعلق بالتصيّد الاحتيالي والبرامج الضارة، عملنا مع مجموعة جهات الاتصال لوضع سير عمل بياني واضح حول ما هو توزيع الأدوار في المراحل المختلفة بين السجلات وأمناء السجلات؟ ما هي قنوات المعلومات وما إلى ذلك؟

يسعدني للغاية أن أذكر هذا هنا لأن جرايم بونتون موجود هنا في الزاوية وقد رآه البعض منكم قبل ذلك. لقد أدى ذلك إلى مبادرتين عظيمتين يسعدني للغاية أنهما تم بناؤهما على أساس العمل الذي تم إنجازه في شبكة عمل الإنترنت والاختصاص القضائي I&JPN، وإنشاء معهد انتهاك نظام اسم النطاق DNS، وذلك بفضل مساعدة سجل المصلحة العامة PIR، والإنتاج ضمن هذا السياق لشيء ناقشناه داخل مجموعة جهات الاتصال، وهي واجهة التبليغ عن الانتهاك، التي تسمى الآن NetBeacon.

لقد كان CleanDNS... كان لجيف بيدسر دور أساسي في تحقيق ذلك. بريان سيمبوليك الجالس بالقرب منه عن سجل المصلحة العامة PIR. برايان في الواقع منسق مجموعة جهات الاتصال التي لدينا في شبكة عمل الإنترنت والاختصاص القضائي I&J. وهذا العمل مذهل بالنسبة لي لأنه نتيجة خمس سنوات من العمل الذي أدى إلى عنصر ملموس للغاية، شيء عملي، وليس مجرد مناقشة أو ورقة. إنه حقًا شيء عملي. وتحية كبيرة لمن يحملون الشعلة إلى الأمام.

هذا مهم لأنه بالإضافة إلى ذلك، أدى ذلك أيضًا إلى المناقشات التي تجري هنا خلال ICANN76 فيما يتعلق بتحسين اتفاقية الاعتماد.

لذلك أنهي هذا الجزء ولدي جزء قصير جدًا بعد ذلك. يتعلق هذا بانتهاك نظام اسم النطاق DNS، الذي نفهمه على أنه العناصر الخمسة التي كنا نتحدث عنها. الشريحة التالية من فضلك. أعتقد، باختصار، أن هناك اتفاقًا بين الجهات الفاعلة المسؤولة على أن انتهاك نظام اسم النطاق DNS، المفهوم بهذه الطريقة، هو بالفعل شيء مبرر بشكل عام للتصرف على مستوى نظام اسم النطاق DNS عندما يكون هناك دليل موثق إلا إذا كان الموقع مخترق أو هناك أشياء أخرى. لكن بشكل عام، نرى الحركة في اتجاه إيجابي نحو تعاون قابل للتنفيذ.

الجزء الأخير الذي أريد أن أتطرق إليه، الذي هو قيد الإعداد في الوقت الحالي، هو مسألة الانتهاك المتعلقة بالمحتوى، التي هي أكثر تعقيدًا لأن الصورة هنا عبارة عن صورة معكوسة قليلًا. بشكل عام، مستوى نظام اسم النطاق DNS ليس المكان المناسب لمعالجة الانتهاك المتعلق بالمحتوى لأسباب عديدة، بما في ذلك حقيقة أنه ليس دقيقًا بدرجة كافية. ومن الصعب أن يكون لديكم شيء يتلاءم مع المخالفات في منطقة أو أخرى.

يختلف الاختصاص لتقييم ما إذا كان هناك انتهاك. وهو ليس شيئًا فنيًا يعرفه المشغلون. وبصفة عامة، فهو ليست أداة فعالة لأن المحتوى يظل متاحًا في معظم الحالات.

لكن يوجد مع ذلك عدد معين من المواقف الاستثنائية بدرجة كافية لتبرير اتخاذ إجراء على مستوى نظام اسم النطاق DNS عند ملاقاتها. وفي المناهج التشغيلية التي أصدرناها في عام 2019، قبل المؤتمر العالمي الذي نظمناه في برلين، هناك أربعة عناصر، مبدئيًا، يمكن وضعها في الاعتبار للتخمين أو التقييم عندما يكون من المناسب التصرف على مستوى نظام اسم النطاق DNS حيال الانتهاك ذات الصلة بالمحتوى.

إلى أي مدى يتم الاتفاق عالميًا على أن المحتوى المعني غير قانوني؟ هنا، لديكم تدريج كامل بين الأشياء – مواد الإساءة الجنسية للأطفال CSAM، على سبيل المثال، من جهة بطريقة معينة والأشياء المتنوعة للغاية من حيث التشريعات حول العالم. تنوع كبير حول ما هو غير قانوني وما ليس كذلك. ونسبة الموقع المخصصة للمحتوى المخالف. والغرض المتعمد أو سوء النية للمسجَّل أو مشغل الموقع. وأيضًا، إن كانت المستويات الأخرى قد استنفدت في التوجه إلى مشغل الموقع أو المسجَّل أو موفر الاستضافة.

لا أتعمق في هذا الأمر ولكن من المهم حقًا التمييز بين هاتين الفئتين من الأشياء. كلاهما مهم لكن لا ينبغي التعامل معهما بالطريقة نفسها تمامًا. أحد التحديات الكبيرة هو أنه ليس لدينا مساحة لمناقشة هذه المشكلة الثانية. وICANN هي المكان المناسب لمناقشة مسألة انتهاك نظام اسم النطاق DNS بالطريقة التي وصفناها من قبل. لكن كان من الواضح جدًا أنها وفقًا للمهمة – والمجتمع يتماشى تمامًا مع هذا – ليست المكان المناسب لمناقشة الانتهاك المتعلق بالمحتوى. كانت هناك منشورات على المدونة باستمرار بخصوص أن "ICANN ليست شُرطة المحتوى،" إلخ. وهذا أمر مفهوم تمامًا.

المشكلة هي أنه لا يوجد أي شيء آخر يمكن مناقشته فيه. هذا هو السبب، في مايو/أيار الماضي 2022، في أن جزءًا كبيرًا من الأشخاص الذين شاركوا في مجموعة جهات الاتصال الخاصة بشبكة عمل سياسة الإنترنت والاختصاص القضائي I&J قد طلبوا منا أن نكون في الأساس المكان الذي يمكن فيه استكشاف مناقشة انتهاك محتوى موقع الويب لتلك الظروف الاستثنائية، وإيجاد العتبات والمعايير والآليات.

هذا هو حيث شرعنا في ذلك هذا العام. وهي خطوة أولية. مجرد بداية. لكني أعتقد أنه من المهم لمجتمع اللجنة الاستشارية الحكومية GAC هذا أن يكون لديه الصورة الكاملة وأن يفهم أن ICANN تمضي قدمًا حقًا على أساس العمل الذي قمنا به بشكل جماعي بشأن مسألة انتهاك نظام اسم النطاق DNS. وهو ليس مثاليًا ويجب تنفيذه ويجب تعزيزه. لكنه يمضي حقًا إلى الأمام في هذا الصدد – وضوح أفضل وآليات أفضل وتعاون أفضل.

فيما يتعلق بالانتهاك المتعلق بالمحتوى، على الرغم من أنه ليست داخل ICANN، فإننا بصفتنا شبكة عمل سياسة الإنترنت والاختصاص القضائي I&JPN نواصل هذا النشاط حول العناصر التالية التي تمثل الشريحة التالية. أولًا، تُثار طبقة نظام اسم النطاق DNS للانتهاك المتعلق بالمحتوى إما لوجود سبب مطلق للاتجاه إلى ذلك مباشرةً أو لأنها الملاذ الأخير بعد استنفاد المستويات الأخرى في المسلسل. والسؤال هو: كيف تتصل بمشغل الموقع، المسجِّل، موفر الاستضافة؟ مسار التصعيد هو المناقشة الأولى.

العنصر الثاني هو كيفية صياغة معايير العتبة. لإعطائكم مثالًا، يمكنكم القول: "يجب تخصيص الموقع بالكامل أو تخصيصه للمحتوى أو النشاط المخالف." أو يمكنكم القول: "لا يوجد محتوى

شرعي آخر على الموقع بخلاف هذا." أو يمكنكم القول: "قصد مشغل الموقع هو تنفيذ س، ص، ع." الصياغات مهمة ونحن نسهل تلك المناقشات.

أخيرًا، يعد مفهوم قابلية الوصول مفهومًا مثيرًا للاهتمام. في اللحظة التي نقول فيها أن هناك مسار تصعيد، كيف ترسل إشعارًا وكيف تتصل بالمسجِّل أو مشغل الموقع أو موفر الاستضافة في هذا الشأن؟ وهذا شيء سنستكشفه بمزيد من التفصيل لأنه لا يوجد مكافئ واضح لنظام WHOIS لموفري الاستضافة. ويعد العثور على مكان استضافة موقع معين أكثر تعقيدًا من مجرد العثور على أمين السجل.

أخيرًا، ذكرت مفهوم اتفاقيات المُخطِر الموثوق به. وهي نقطة مهمة للغاية لأنه على وجه الخصوص بالنسبة للانتهاك المتعلق بالمحتوى – حتى أكثر من ذلك المتعلق بالتصيّد الاحتيالي ولكن الانتهاك المتعلق بالمحتوى – لن يكون هناك حل لهذا الأمر بدون التعاون بين الفئات الثلاث للجهات الفاعلة – سلطات إنفاذ القانون، والمُخطِرين من الأنواع المختلفة الذين يجب أن يزيدوا من قدراتهم ومصداقيتهم ومشغلي نظام اسم النطاق DNS في الاتفاقيات الحالية.

كتلاعب بالألفاظ لمن يتذكرون صياغة تأكيد الالتزامات بين الإدارة القومية للاتصالات والمعلومات في الولايات المتحدة NTIA وICANN في الأيام الخوالي، أعتقد أن هناك مفهوم إطار عمل وهو تأكيد الالتزامات المتبادل. ونحتاج إلى آليات تجمع المُخطِرين ذوي الكفاءة وإجراءات العملية الواجبة، وإنفاذ القانون الذي يسهل التعاون، والمشغلين للتعامل مع الحالات عندما يكون من المناسب التصرف على مستوى نظام اسم النطاق DNS.

أريد أن أوضح أن ما نتحدث عنه هنا ليس التعامل مع لائحة المنصات الكبيرة. ليس Facebook. وليس Twitter في هذا العالم. لن تطلب إزالة Facebook.com نظرًا لوجود محتوى ما في إحدى المجموعات الفرعية الموجودة عليه. لكن عندما يُنشئ شخص ما موقع ويب خلف اسم نطاق له نية خبيثة، فإن العثور على هؤلاء الأشخاص وإيقاف ممارسة الضربة القاضية بشكل أساسي المتمثل في إيقافه هنا ثم إيقافه هناك، والتحرك نحو اصطياد الأشخاص الذين هم بالفعل ينفذون هذه الأشياء هو التعاون المهم المطلوب.

وخلاصتي هي أن هذه مسؤولية مشتركة. وهذا شيء يتطلب التعاون بين مختلف الجهات الفاعلة. ويتمثل شعار شبكة عمل سياسة الإنترنت والاختصاص القضائي في "تمكين التعاون بين أصحاب المصلحة المتعددين." ونقوم بذلك لتسهيل صياغة عدد معين من الاتفاقيات. ونحن سعداء جدًا

لأنه أدى إلى تقدم داخل منظومة ICANN. وهذه هي الطريقة الوحيدة التي يمكننا من خلالها معالجة هذه القضايا.

لديكم، في الشرائح، سلسلة... لا، يجب أن توجد شريحة قبل ذلك. واختفت. سأعيد دمجها. هناك شريحة بها جميع الوصلات والروابط الخاصة بالوثائق التي قدمتها. في الشريحة الأخيرة، هذه تفاصيل جهة الاتصال الخاصة بي وجهات الاتصال مع أجيث فرانسيس، إذا أردتم التحدث إلينا بشأن هذا بعد ذلك. شكرًا جزيلًا لإتاحة الفرصة لهذا العرض.

منال إسماعيل: شكرًا جزيلًا يا برتراند، على العرض التقديمي الشامل للغاية والمنظم جيدًا والغني بالمعلومات. قبل تسليم الكلمة إلى قادة موضوعات اللجنة الاستشارية الحكومية GAC، أريد فقط إعطاء الكلمة ليد مرفوعة منذ مدة طويلة في Zoom من ممثل إيران. هل تريد أن تنطلق أولا؟ حسنًا. يا كافوس، ثانية فقط. كريس وبعد ذلك سأعطيك الكلمة. أعتذر.

كريس لويس-إيفانز: شكرًا يا منال. كنت سأقدم اقتراحًا فقط، في الواقع. لقد تلقينا الكثير من المدخلات، ويتحدث كثيرون منا. ربما، إذا كان لديكم أي أفكار أو أي أسئلة لنا حول العرضين الأخيرين، فسيكون ذلك موضع ترحيب الآن. ثم سنغطي الأنشطة الجارية داخل مجتمع ICANN والاعتبارات الخاصة بلغة البيان الرسمي في كانكون. فهذا سيكون له أسئلة أيضًا. ولكن ربما في العرضين التقديميين الأخيرين اللذين قمنا بهما، ستكون بعض الأسئلة والأفكار جيدة الآن. شكرًا.

منال إسماعيل: شكرًا جزيلًا يا كريس. يا كافوس، أي شيء في الجزء الأول من هذه الجلسة، إما إلى قادة الموضوعات أو إلى برتراند؟ أرجو أن تتفضل.

كافوس أراستيه: شكرًا جزيلًا يا منال. اسمحوا لي أن أعرب عن خالص تقديري للأشخاص على المنصة. كان ذلك، في رأيي، أحد أكثر المناقشات إثارة للاهتمام التي أجريناها حول انتهاك نظام اسم النطاق

DNS. وعلى الرغم من أنني لا أريد إجراء مقارنة بين الاختلافات، إلا أن الجزء الأخير، بالنسبة لي، كان ممتعًا للغاية.

كما ذكرت بالأمس، لدينا مشاكل. وقمنا بحل المشاكل. الرئيسة الموقرة، ما أوصي به أولًا، أنت ونيكول، رئيس اللجنة الاستشارية الحكومية GAC القادم، نحتاج إلى وضع جدول أعمال اللجنة الاستشارية الحكومية GAC للاجتماع القادم وإعطاء وقت أكثر لهذا الموضوع. ليس من الممكن، ظاهريًا، أن نزور شيئًا ما ولا ننفذ إلى قلب المشكلة كما فعلنا اليوم لنرى ما نحن عليه. وهناك أشياء كثيرة [أمامنا]. لا أدري. ليس لدينا وقت الآن لأشرح ذلك. لدي بعض الاقتراحات. ولا أعرف ماذا تقترحون عليّ. لكن يوجد طريق للمضي قدمًا.

لكني أعتقد أنني أريد أن أتناول نقطة واحدة فقط. ذكر الصديق الموقر على الجانب الأيمن من المنصة التعاون الحكومي الدولي. ونوقش هذا سنوات عديدة. إنها ليست قضية ICANN لأن ICANN ليست حكومية دولية واللجنة الاستشارية الحكومية GAC ليست حكومية دولية. اللجنة الاستشارية الحكومية GAC هي لجنة استشارية حكومية. أما الحكومات فهي حكومية دولية. هم في مكان آخر ولكن ليس هنا.

وأعتذر. أنا [صريح جدًا] مع الجميع. في كثير من الأحيان، أردنا معالجة هذه المسألة، التعاون الحكومي الدولي. وعارضت بعض الحكومات ذلك، معتبرة أن الجرائم الإلكترونية قضية وطنية ولا ينبغي التعامل معها دوليًا. وقالوا إن أي تعاون حكومي دولي يمكن أن يكون مفيدًا إذا [دخلتم] في معاهدة. وليس من الممكن أن يكون هناك اتفاق على ذلك.

لذا دعونا نتطرق إلى عمق الموقف، وليس في هذه الجلسة لأننا في نهاية الاجتماع. رئيسة اللجنة الاستشارية الحكومية GAC الموقرة، دعونا، إن أمكن، نناقش المشكلة أكثر قليلًا لنرى ما يمكننا القيام به. وتم طرح العديد من النقاط الجيدة. وما أثير حتى الآن هو في الغالب يثير المشاكل. لكن مع ذلك، لم يتم اقتراح الحلول. وهذا مهم. أقول في بعض الأحيان، لا يوجد أسهل من طرح المشاكل. لكن من الصعب اقتراح حلول. أين الحلول؟

علينا أن نتبنى نهجًا عمليًا أكثر، وليس الجزء التشريعي لنرى ما يمكننا القيام به. ونصنفها، حسب درجة الأولوية، ما يمكننا القيام به. وليس من السهل معالجة التعاون بين الحكومات في الوقت الحاضر. ولكن هناك العديد من الأشياء الأخرى التي يجب معالجتها وما إلى ذلك.

لقد تلقينا تقارير من المملكة المتحدة والولايات المتحدة الأمريكية. يمكننا أن نسأل جميع أعضاء اللجنة الاستشارية الحكومية GAC، "هل لديكم نفس الخبرة؟ ما هو التقرير؟ هل واجهت...؟ " لقد واجهت ولكني لم أبلغ. أنا شخصيًا، عبر بريدي الإلكتروني عدة مرات... قلت ذلك بالأمس. كان هناك [شخص آخر] يقول [كان لديهم سيارة دبلوماسية] بنسبة 10% من السعر. لم أفتح ذلك لأن ابني ذكي جدًا. وقال لي: "أبي، لا تفتح أيًا من هذه الأشياء. لا تفتحها. إذا تلقيت بريدًا إلكترونيًا، وأنت لا تعرف المرسل، فلا تفتحه. قد لا أكون جيدًا، لا [غير مسموع]. لكن لا تفتح ذلك لأنك قد تكون على الفور ..."

ثم هناك أساليب أخرى. بعض موفري خدمة البريد الإلكتروني لديهم أمن مزدوج، وهو أنه إذا تم أخذ كلمة المرور الخاصة بك وما إلى ذلك من قِبل شخص ما، باستثناء سطح المكتب أو الجهاز، فلن يتمكن أحد من استخدام ذلك لأنهم يسألونهم عن الطريقة الثانية – الأمن الثاني. لذلك علينا تقديم بعض النصائح الجيدة للأشخاص كإجراء وقائي أولي. ما هي تلك الأشياء التي على الأقل تقلل مقدار هذا؟ لذلك هذا شيء يجب أن نناقشه.

هناك العديد من الأشياء الأخرى التي أود طرحها ولكن ليس هناك وقت. وأعتذر إذا كنت [غير مسموع] لكن هذا كل شيء. شكرًا.

منال إسماعيل: شكرًا جزيلًا لممثل إيران. إذا سمحت لي يا كريس، لدينا طلبان آخران للتحدث وربما يمكنك الرد قليلًا. أمامنا 20 دقيقة فقط متبقية ولدي ممثل جمهورية الكونغو الديمقراطية ثم ممثل الولايات المتحدة. أرجو أن تتفضل. ممثل جمهورية الكونغو الديمقراطية، من فضلك.

بليز أزيتمينا فوندجي: شكرًا جزيلًا. شكرًا لجميع المتحدثين على المنصة. أود حقًا، مثل كافوس، أن أذكر مدى أهمية هذا العرض التقديمي. من وجهة نظر الحكومة، بالنسبة لمعظم الحكومات ومعظمها من إفريقيا، أعتقد أن توقعات حكومتنا بوجود مندوب داخل اللجنة الاستشارية الحكومية GAC هي بشكل أساسي لمعالجة هذا النوع من الانتهاكات.

سيكون سؤالي أو تعليقي بشكل أساسي، بطبيعة الحال، من الواضح أن العنوان أو الموضوع هنا هو الانتهاك. لكني أود حقًا أن أسأل عما إذا كان هناك أي إجراءات يمكن أن تتخذها الحكومات

لمنعه. بالطبع، نتحدث عن الشفاء، عن العلاج. لكن كما تعلمون، نقول بالفرنسية: "الوقاية خير من العلاج." هل هناك بعض الإجراءات التي يمكن أن تنصح ICANN بها؟

بالطبع، نتحدث عن قضايا الأمن السيبراني حيث يتعلق الأمر بسيادة الدول. لكن حتى فيما يتعلق بالنصائح، خاصة للشركات ومعظمها للحكومات، ما هي النصائح؟ كيف يمكننا منع حدوث ذلك؟

لقد رأينا بعض العروض التقديمية من مكتب التحقيقات الفيدرالي ومعظمها أيضًا من تجربة المملكة المتحدة. أفهم أن هناك بعض الدراسات. هناك بعض الإحصائيات التي قد تساعد في فهم سبب تعرضنا لهذا النوع من الانتهاك. ونعلم أنه بالنسبة إلى المستخدمين النهائيين، فإن الأمر يتعلق بالتصيّد الاحتيالي بشكل أساسي. إنها مراسلة بريد إلكتروني، اختراق كلمة مرور. ولكن بالنسبة للشركات ومعظم الحكومات، هل هناك بعض الإجراءات التي يمكن القيام بها للوقاية منها بدلًا من انتظار الشفاء أو العلاج من الانتهاك؟ شكرًا.

منال إسماعيل: شكرًا جزيلًا لممثل الكونغو. عندي ممثل الولايات المتحدة وممثل فرنسا، من فضلكم، باختصار شديد. سأسلم الكلمة لكريس. ممثل الولايات المتحدة، تفضل.

سوزان شالمرز: شكرًا جزيلًا منال. يسعدني حقًا التنازل عن الكلمة حتى يمكن الإجابة على سؤال زميلنا. شكرًا.

منال إسماعيل: شكرًا جزيلًا لممثل الولايات المتحدة. لدي فرنسا ومن ثم سأسلم الكلمة لك. هل هذا جيد يا "كريس"؟ ممثل فرنسا، تفضل.

جوناس راوولي: بادئ ذي بدء، اسمحوا لي أن أشكر جميع أعضاء اللجنة على عروضهم التقديمية. ويشرفني أن أكون هنا لأحل محل زميلي السابق. أردت فقط أن أتدخل، للمساهمة في المناقشات. أنا جديد في اللجنة الاستشارية الحكومية GAC ولدي انطباع أنه قبل البدء في العمل، يجب أن أتعلم المزيد عن موضوعات معينة.

أولًا، بصفتي وافدًا جديدًا، أود استكشاف بعض الوسائل المساعدة لمعرفة ما إذا كان بإمكاني فعل شيء لمنع الهجمات الخارجية. أشعر أن السعر المميز الذي تقترحه بعض الجهات الفاعلة يؤدي إلى انتهاك ما في نظام اسم النطاق DNS. لذا أود أن أعرف كيف يمكننا العمل لمعرفة سعر تجديد أسماء النطاقات. ربما يمكن أن يساعد هذا المجتمع في فعل شيء حيال ذلك.

نعرف الجهات الفاعلة التي لا تعمل بشكل قانوني. لذلك ربما يمكننا الكشف عن بعض الآليات التي يستخدمونها. لكن بعض الصعوبات التي نلاحظها تحتاج إلى إثبات بالأدلة. وأعتقد أن هذا شيء نحتاجه. شكرًا لكم على اهتمامكم.

منال إسماعيل: نوجه الشكر لممثل فرنسا. أرى يد ممثل رواندا مرفوعة. هل يمكنك أن تجعل الأمر مختصرًا جدًا لأن الوقت ينفد.

فينسنت موسمينالي: شكرًا جزيلًا. أود فقط أن أشكر مقدمي العروض وأعضاء اللجنة الذين قدموا العرض التقديمي لتقرير الولايات المتحدة وتقرير المملكة المتحدة عن الجرائم الإلكترونية. فقط للحصول على بعض التوضيح [غير مسموع] العملات المشفرة. يواجه معظم الأشخاص الآن بعض التحديات المتعلقة بالنطاقات ذات الصلة التي تستخدم الجرائم الإلكترونية [المرتبطة] بالعملات المشفرة. وتغلق هذه النطاقات أحيانًا ويفقد الأشخاص [غير مسموع] أموالهم واستثماراتهم. وعليهم [الآن] متابعة ذلك الاستثمار. أود فقط أن أعرف كيف يتعاونون مع الإنتربول. شكرًا.

منال إسماعيل: شكرًا جزيلًا لممثل رواندا. نعود إليك يا كريس. أعتذر للضغط عليك في الوقت المحدد لكن من الجيد أن تسمع من زملائك في اللجنة الاستشارية الحكومية GAC. أرجو أن تتفضل.

كريس لويس-إيفانز: شكرًا يا منال. بالتأكيد وأشكركم شكرًا جزيلًا على إسهاماتكم. سأحاول تلخيص بعض مدخلاتي بسرعة كبيرة. فيما يتعلق بالنصائح، التي سمعناها من كل من الكونغو وفرنسا، فلن نغطي ذلك هنا الآن. هناك الكثير من النصائح. وهناك الكثير من الأشياء التي يمكنكم القيام بها. ربما تكون

هذه مادة لورشة عمل بناء قدرات في ICANN في المستقبل. وربما تكون جلسة واحدة لتنظر فيها اللجنة الاستشارية الحكومية GAC لأنها ستحتاج إلى أن تكون جلسة أطول قليلًا. قد يكون هذا شيئًا يمكننا التفكير فيه.

ثم، فيما يتعلق بنقطة ممثل إيران حول المبادرة الاستباقية: "ماذا يمكننا أن نفعل؟" أعتقد أن برتراند غطى اثنين من هؤلاء. NetBeacon، الذي تم ذكره بالتأكيد كأداة لإعداد التقارير، هو طريقة عمل وطريقة لمكافحة بعض من ذلك. وهذا يقودنا بشكل جيد إلى الأنشطة الجارية، إذا تمكنا من الانتقال إلى تلك الشرائح. سنغطي بعض الإجراءات التي كانت تجري في المجتمع والتي تدعم بعضًا من انتهاك نظام اسم النطاق DNS.

من ناحية العملات المشفرة أيضًا، أعتقد أن هذا يتعلق بنقطة برتراند قليلًا أيضًا. يمكن تقديم ذلك إما من بريد إلكتروني للتصيّد الاحتيالي، حيث يقع في انتهاك نظام اسم النطاق DNS، أو قد يكون مشكلة متعلقة بالمحتوى، حيث يقع ضمن الآليات الموجودة هناك.

انتقل إلى الأنشطة المجتمعية. هناك الكثير من العمل الجاري. وتعمل السجلات على المشاركة الطوعية للإحصاءات. كما رأينا من منظور إنفاذ القانون، نعتقد أن هذا مهم جدًا. ويعطينا صورة شاملة. وبالمثل بالنسبة للسجلات التي من شأنها أن تدعم ذلك.

فقط لأذكر النقطة التالية، وهي acidtool.com. قال برتراند إنه لا توجد أداة لتحديد موفري خدمات الاستضافة والبريد الإلكتروني. في الواقع، أنشأ أمناء السجلات هذه الأداة لمساعدة الأشخاص على تحديد النقطة الدقيقة والصحيحة للدخول إليها واتخاذ إجراءات فعالة. وسمعنا من عرض شبكة عمل سياسة الإنترنت والاختصاص القضائي I&J أن اتخاذ إجراءات فعالة أمر مهم حقًا. وتحديد تلك النقطة الصحيحة، سواء كان بائعًا وسيطًا أو أمين سجل أو سجلًا أو موفر استضافة، فذلك يعد أمرًا مهمًا حقًا.

نداء آخر لـ NetBeacon، مرة أخرى، هنا، كطريقة لاتخاذ إجراء. ويتماشى هذا تمامًا مع التوصيات داخل اللجنة الاستشارية للأمن والاستقرار SSAC115. لقد حصلنا على عرض تقديمي جيد من اللجنة الاستشارية للأمن والاستقرار SSAC حول ذلك، ومرة أخرى، ورد ذكره في تقرير شبكة عمل سياسة الإنترنت والاختصاص القضائي I&J. هذه كلها أنشطة تساعد في الحدّ من تلك [النصيحة] الجارية في الوقت الحالي. يشارك أيضًا معهد انتهاك نظام اسم النطاق

DNS عمله التحليلي من البيانات التي تم جمعها والنظر إليها كجزء من التبليغ عن انتهاك نظام اسم النطاق DNS. الشريحة التالية من فضلك.

ربما أتحدث بسرعة كبيرة بالنسبة للمترجمين الفوريين، لذا أعتذر الآن وأبطئ قليلًا. كما كان فريق المنظمة الداعمة للأسماء العامة GNSO الصغير المعني بانتهاك نظام اسم النطاق DNS نشطًا للغاية. أريد فقط أن أشير هنا إلى أن النتائج التي توصلوا إليها تعكس بعض مشكلاتنا ذات الأهمية في بيان لاهاي بأن أي عمل لعملية وضع سياسات PDP مستقبلية بشأن انتهاك نظام اسم النطاق DNS يجب أن يكون مصممًا بشكل ضيق لإخراج بعض النتائج العملية في الوقت المناسب. ومن وجهة نظر ممثل إيران، يجب استهداف أي عمل نقوم به في المجتمع لتمكينه من الحدوث والسرعة. وأعلم أن هناك إحباطات في بعض الأحيان بشأن الأشياء التي لا تحدث بالسرعة الكافية. الشريحة التالية من فضلك.

أيضًا ضمن اختصاص ICANN، عندهم فريق مكتب المدير الفني المسؤول OCTO، ولديهم نظام التبليغ عن نشاط انتهاك النطاق DAAR. سمعنا عن ذلك أيضًا يوم السبت، وأعتقد أنه كان حوله، يقومون بتحليل بيانات 1145 من نطاقات gTLD، فعدد النطاقات الموجودة كان مفاجئ. كما أعتقد أن هناك 21 من نطاقات المستوى الأعلى لرمز البلد ccTLD. مرة أخرى، إنها مجرد صورة أفضل لإعطاء فهم أكبر لما يحدث للقدرة على اتخاذ إجراءات فعالة. الشريحة التالية من فضلك.

هذا مجرد تذكير بشأن هذا المسار ومن يجب الاتصال به. وهي مساحة معقدة. هذا مخطط ICANN فشكرًا جزيلًا لكم. لا يمكنني الرسم في أي مكان قريب مثل ذلك على الإطلاق. نسمع عن التوجه إلى الشخص المناسب حتى نتمكن من اتخاذ الإجراء الصحيح في الوقت المناسب. بالتأكيد، من وجهة نظري، نرى أين يمكننا القيام بذلك، وهذا أيضًا يقلل من الضرر. لذا فإن القدرة على فهم إلى أين نذهب وأين نذهب بسرعة أمر مهم حقًا. وأدوات مثل NetBeacon وACID Tool مفيدة حقًا.

الصورة في الواقع أكثر تعقيدًا من هذا أيضًا. على الجانب الأيمن، لديك المسجِّل ثم بائع وسيط. لا يوجد دائمًا بائع وسيط أو في بعض الأحيان يوجد أكثر من بائع وسيط. لذا فإن فهم ذلك أمر مهم حقًا لتكون قادرًا على العثور على المكان المناسب للتوجه إليه. الشريحة التالية من فضلك.

فقط للإشارة إلى جبهة البائع الوسيط، أثناء المرحلة 1 من العمل على العملية المعجّلة لوضع السياسات EPDP، أوصت أنه يجب على أمناء السجلات إنشاء عنصر بيانات للبائع الوسيط بعلاقة مع المسجَّل. وهذا مهم حيث يوجد العديد. لذلك ضمن استجابة نظام WHOIS في الوقت الحالي، يوجد حقل بائع وسيط ولكن ليس بالضرورة جمع كل هؤلاء. وكما قلت، من المهم حقًا بالنسبة لنا أن نكون قادرين على الانتقال مباشرة إلى الشخص الذي يمكنه إجراء الاستجابة الأكثر فاعلية. وقد انعكس ذلك أيضًا في مراجعة المنافسة وثقة المستهلك وخيار المستهلك CCT. الشريحة التالية من فضلك.

وأسلم الكلمة إلى لورين. أعتذر عن السرعة ولكني أردت الوصول إلى المجموعة الثانية من الأسئلة إن استطعنا.

منال إسماعيل: يا لورين، لدينا بالفعل طلب للكلمة. هل تريدين منا أن ننتقل إليه أولًا؟ حسنًا. أرى يد ممثل المملكة المتحدة مرفوعة. تفضل يا نايجل.

نايجل هيكسون: شكرًا جزيلًا سيدتي الرئيسة. سأكون سعيدًا أن ننتقل إلى لورين أولًا ثم نعلق لاحقًا، ربما. تفضلي يا لورين.

لورين كابين: شكرًا يا نايجل. أتحدث بصفتي أحد الرؤساء المشاركين لمجموعة عمل السلامة العامة وأحد الخبراء المتخصصين في هذا الموضوع المهم للغاية. هل يمكننا الانتقال إلى الشريحة التالية؟

يسعدني أن الجلسة كانت تفاعلية، وحتى قبل هذه اللحظة. لكن كان هناك الكثير من المناقشات، ووجهات النظر، والمعلومات حول ما تود اللجنة الاستشارية الحكومية GAC أن... دعوني أعيد الصياغة. كان هناك الكثير من المعلومات ووجهات النظر المشتركة. والآن وصلنا إلى النقطة التي يمكننا فيها مناقشة ما تود اللجنة الاستشارية الحكومية GAC تسليط الضوء عليه في البيان الرسمي، وبالتالي المشكلات المحتملة.

بادئ ذي بدء -- وهذا يقع ضمن فئة "إذا كان الأمر يستحق القول، فإنه يستحق القول عدة مرات" -- لدينا مفاوضات العقد الجارية بين السجلات وأمناء السجلات وICANN. مرة أخرى، الهدف الكامل لهذه العملية هو رفع الحد الأدنى، وذلك لتحسين التزامات العقد فيما يتعلق باتخاذ إجراءات ضد انتهاك نظام اسم النطاق DNS. الالتزامات، وليس الجهود الطوعية. هذه الالتزامات، سيكون الهدف أن نعكس التزام سيغطي الجميع. ونأمل أن يشمل ذلك جهات فاعلة سيئة وأن يمنح ICANN أيضًا أدوات أكثر مما لديها بالفعل للتعامل مع تلك السيناريوهات التي تتعلق بانتهاك نظام اسم النطاق DNS.

مرة أخرى، هذه مجرد خطوة وقد تكون هناك خطوات مستقبلية. لكن قد يكون هذا وقتًا مهمًا للجنة الاستشارية الحكومية GAC للإقرار والإشادة بأن هذا الجهد مستمر وأنه تم تنفيذه بمبادرة من الأطراف المتعاقدة. وهذه خطوة استباقية ويجب أن تكون محل ترحيب دائمًا.

هذه هي الخطوة الأولى من خطوات عديدة حتى يجري تصور عمل السياسة في المستقبل. وأريد أن أكرر أحد التعليقات التي أدلى بها زميلي من إيران بأنه من المهم جدًا إعطاء الأولوية هنا والتركيز لأن هذه هي الطريقة التي يتم بها إنجاز الأمور. ويمكننا تطبيق هذين المبدأين التوجيهيين على أي عمليات لوضع السياسات PDP، التي لم تكن معروفة بالضرورة بإجراءاتها السريعة والمركزة ولكن يمكن أن تكون كذلك ويجب أن تكون في هذا السياق. أيضًا، قد تكون هناك فرص لمزيد من المفاوضات بين الأطراف المتعاقدة وICANN.

وللتنبيه هنا، ستكون هناك فرصة قادمة للتعليقات العامة بمجرد أن تطلق الأطراف المتعاقدة ثمار عملها، وهو ما ننتظره بفارغ الصبر. ثم ستكون هناك فرص للجنة الاستشارية الحكومية GAC لتقرير نوعًا ما المدخلات التي ترغب في بثها. الشريحة التالية من فضلك.

وتم تحديد قضية من البائعين الوسطاء أيضًا. السبب الذي يرتبط بانتهاك نظام اسم النطاق DNS هو أنه مهم للغاية، كما أشار زميلنا برتراند من شبكة عمل سياسة الإنترنت والاختصاص القضائي. من المهم جدًا أن تكون قادرًا على التوجه إلى الكيان الصحيح عندما تتعامل مع انتهاك نظام اسم النطاق DNS. كان هذا الموضوع موضوع مدخلات اللجنة الاستشارية الحكومية GAC بالعديد من الصيغ المختلفة، والمرتبط بالتقرير النهائي للمنافسة وثقة المستهلك وخيار المستهلك CCT، ومؤخرًا أيضًا، توصيات بيانات تسجيل النطاق المرحلة 1. الشريحة التالية من فضلك.

والآن أعود إلى زملائي في اللجنة الاستشارية الحكومية GAC للحصول على مساهماتهم فيما يتعلق بالرؤى والأفكار حول ما يمكن أن يدخل في البيان الرسمي للجنة الاستشارية الحكومية GAC. أعلم أن الوقت قصير، وأشير أيضًا أن لدينا جلسات صياغة البيان الرسمي. ولكن سيكون هذا وقتًا رائعًا للحصول على معاينة لما يفكر فيه الأشخاص.

منال إسماعيل: شكرًا جزيلًا يا لورين. لدينا ممثل المملكة المتحدة وممثل إيران وممثل المفوضية الأوروبية. وأمامنا ثلاث دقائق لذلك آمل... يُرجى الإيجاز. ممثل المملكة المتحدة، تفضل.

نايجل هيكسون: نعم. شكرًا جزيلًا يا منال. شكرًا جزيلًا للأشخاص الموجودين على المنصة على عروضهم. لقد كانت جلسة مفيدة بصورة استثنائية، كما أشار أعضاء اللجنة الاستشارية الحكومية GAC الآخرون. أربع نقاط سريعة فقط، إذا جاز لي ذلك.

الأولى هي إعادة التأكيد على موقفنا بشأن استمرار مفاوضات العقد. وهذا إيجابي جدًا. الجلسة التي أجريناها بالأمس مع الممثلين من أمناء السجلات والسجلات، أرى أنها كانت ممتازة. وبالتأكيد نتطلع إلى التشاور العام. ولا نية للتدخل في تلك المفاوضات على الإطلاق. إنما نتطلع إلى التحديثات بالطبع. وكما قال الممثلون أمس، هذه خطوة أولى. قد تكون هناك مبادرات أخرى – عمليات وضع سياسات PDP مصغرة أو أيًا كان – للنظر في انتهاك نظام اسم النطاق DNS.

ثانيًا، فيما يتعلق بالبيان الرسمي، لا شك أننا سنناقش هذه القضايا. وأعتقد أنه من المناسب لنا فقط أن نكون واضحين جدًا في البيان الرسمي حول كيفية ترحيبنا بهذه المبادرات لكن أيضًا تفصيل تلك التوصيات – مشورة اللجنة الاستشارية الحكومية GAC بشأن التوصية 17 من مراجعة المنافسة وثقة المستهلك وخيار المستهلك CCT وغيرها من القضايا المتعلقة بالبائعين الوسطاء الذين تحدثنا عنهم. ويجب أن ننبه لذلك حتى يفهم المجتمع بأكمله أن هناك إجراءات معينة ليعمل بها يجب اتخاذها قبل العملية التالية للإجراءات القادمة SubPro لنطاقات gTLD الجديدة. وأكتفي بهذا القدر. شكرًا جزيلًا.

منال إسماعيل: شكرًا جزيلًا لممثل المملكة المتحدة. لدي ممثل إيران بعد ذلك وسأغلق قائمة الانتظار بعد ممثل اليابان، من فضلك. والآن نستمع إلى ممثل إيران.

كافوس أراستيه: شكرًا جزيلًا يا منال. لقد ناقشت مع بعض الزملاء المميزين، بمن فيهم أنت، أن قضية انتهاك نظام اسم النطاق DNS هي القضية الأساسية في المستقبل القريب والبعيد أمام ICANN. وذلك شيء مهم. لكن الجميع – مجلس الإدارة ومؤسسة ICANN والأعضاء والجميع – يدرسون هذه المسألة. وليست هناك حاجة للحصول على أي مشورة من اللجنة الاستشارية الحكومية GAC بشأن ذلك. دعوا الأشخاص يعبرون عن أنفسهم، ويفكرون في الأمر، ويستوعبون الأمر، ولا ندفعهم أكثر مما نحتاج إلى القيام به. فهم يعرفون ماهية المشكلة.

ومن ناحية أخرى، في القضايا المهمة بالنسبة إلى اللجنة الاستشارية الحكومية GAC، فإن أول شيء نحتاج إلى ذكره هو الاعتراف بالمفاوضات الجارية داخل مجلس إدارة ICANN أو ICANN والأطراف المتعاقدة والسجلات وأمناء السجلات، وهي خطوة طيبة – لنقل ذلك. وبعد ذلك يجب أن نذكر أننا بحاجة إلى تقرير مرحلي حول ذلك في اجتماع ICANN القادم، ICANN77 في واشنطن العاصمة – تقرير مرحلي عما يجري.

ونتوقع أن يكون التقرير النهائي إما في اجتماع 78 أو 79 أو 80 لكن مع وجود تدابير كافية أيضًا، من أجل تقديم المشورة للحكومة أو أفراد اللجنة الاستشارية الحكومية GAC حول كيفية المواجهة، وكيفية المكافحة، كما ذكر زميلي، أو كيفية مواجهة هذا الموقف، والاطلاع على العديد من العناصر الأخرى التي تمت الإشارة إليها في تقارير كريس، لورين، غابرييل – تضمين القضايا المهمة للجنة الاستشارية الحكومية GAC.

وذلك مع محاولة التأكيد على أهمية ذلك الشيء. والعمل على النص ليكون أكثر وضوحًا، وأن يكون أكثر دقة وإيجازًا أيضًا، ومحاول [وضع النقاط] واتخاذ إجراء متابعة. لكنني أقترح عدم تضمين أي شيء يتعلق بانتهاك نظام اسم النطاق DNS في مشورة اللجنة الاستشارية الحكومية GAC في هذه المرحلة. شكرًا.

منال إسماعيل: شكرًا جزيلًا لممثل إيران. لدي ممثل المفوضية الأوروبية، ثم ممثل اليابان. وأذكر بلطف أن يُرجى الإيجاز. ممثل المفوضية الأوربية، تفضل. تفضلي يا جيما.

جيما كاروليلو: شكرًا جزيلًا يا منال. لقد أثنيت على ما تم تقديمه لنا في الدردشة، لذا لن أفعل ذلك مرة أخرى لصالح الوقت. فيما يتعلق باختصار شديد بالنقاط والاعتبارات الخاصة بالبيان الرسمي، كما طلبت لورين بلطف، فإننا نتفق بالتأكيد على أن هذه خطوة رائعة. المفاوضات، ظللنا ندعو إلى إليها لفترة طويلة داخل اللجنة الاستشارية الحكومية GAC. لذلك هذا شيء، بالتأكيد، يجب أن ندعمه.

فيما يتعلق بالمواد الإضافية، قد نرغب في إضافة قسم انتهاك نظام اسم النطاق DNS تحت القضايا ذات الأهمية. سوف يستوعبونه، لكن بالطبع، لمزيد من المناقشة. أولًا وقبل كل شيء، أهمية وجود تدبير وقائي. نحن قلقون بعض الشيء من أن ما سمعناه حتى الآن، يتعلق في الغالب بتدابير رد الفعل. لكن منع انتهاك نظام اسم النطاق DNS أمر أساسي حقًا من وجهة نظرنا. وسمعت ذلك سابقًا أيضًا من زميل أو اثنين. بعد ذلك، ربما يمكنكم استكشاف مسألة الحوافز، التي أثيرت في النصائح الجيدة جدًا من الزملاء من مجموعة عمل السلامة العامة PSWG، وما إلى ذلك، ومن المواقع.

وأخيرًا وليس آخرًا، بالارتباط بما قاله نايجل فيما يتعلق بالجولة القادمة لنطاقات gTLD، بشكل عام، نود التأكد من عدم نسيان العمل السابق – على وجه الخصوص، فيما يتعلق بالإجراءات المعقولة لمنع انتهاك نظام اسم النطاق DNS. لكن اللجنة الاستشارية الحكومية GAC كانت قوية جدًا في ربط دقة البيانات ودقة تسجيل اسم النطاق وانتهاك نظام اسم النطاق DNS في البيانات الرسمية أرقام 71 و72 و73، وأنا متأكدة من وجود المزيد. ولا يتعلق الأمر بإدراج ذلك ولكن فقط لتوضيح النقطة التي نرغب في إنجاز العمل عليها فيما يتعلق بدقة بيانات التسجيل وأهمية منع انتهاك نظام اسم النطاق DNS. شكرًا جزيلًا.

منال إسماعيل: شكرا جزيلا لك يا ممثل مفوضية الاتحاد الأوروبي. وأخيرًا وليس آخرًا، لدي ممثل اليابان بالطبع.

نوبو نيشيغاتا: شكرًا جزيلًا يا منال والرؤساء المشاركين لمجموعة عمل السلامة العامة PSWG. ليلة سعيدة في الواقع. خيم الليل بالفعل في اليابان. فصباح الخير ومساء الخير للجميع من طوكيو. شكرًا جزيلًا على التنظيم الذي أنجز هذه الجلسة الرائعة اليوم.

أريد فقط الرد على العرض الذي قدمته لورين حول الاعتبار للبيان الرسمي. وتود اليابان التعبير عن دعمها لمفاوضات العقد الجارية، وهو أمر محل ترحيب للغاية – التقدم الحالي حتى الآن.

ولكن من ناحية أخرى، تود اليابان طرح سؤال واحد ومسألة واحدة بين اتفاقية اعتماد أمين السجل، المادة 3.18.1، التي تتعلق بالإجراء المطلوب من أمين السجل للتبليغ عن الأنشطة غير القانونية. [لقد أبلغت] الحكومة اليابانية وهي تدرك أن بعض أمناء السجلات لا يتخذون أي إجراء أو حتى لا يستجيبون لتقرير الأنشطة غير القانونية من الأطراف اليابانية. ولهذا السبب تواصل الحكومة اليابانية طلب تحسين نص العقد أو شروطه.

كانت هناك بعض الأدلة من الحكومة اليابانية. ولكن لا تزال هناك مجموعة من الأدلة الأخرى المشابهة لذلك – تقرير تدقيق ICANN أو التقرير الأخير من ICANN والمنظمة الداعمة للأسماء العامة GNSO والأطراف. هذه هي النقطة، فقط أقول إن اليابان تتطلع إلى رؤية مسودة التقرير القادم. بالطبع، سنكون سعداء بالمناقشة بين الجلسات، إذا لاح لنا بعض التقدم.

وبالطبع، في النهاية، لا بد لي من الإعراب عن تقديري الكبير للجلسة السابقة التي قدمت لنا آخر المستجدات بشأن مفاوضات العقد. ونحن على استعداد لمواصلة المناقشة – يسعدنا إجراء مناقشة معكم. شكرًا جزيلًا.

منال إسماعيل: شكرًا جزيلًا لممثل اليابان. وشكرًا جزيلًا يا برتراند، من شبكة عمل سياسة الإنترنت والاختصاص القضائي، غابي، كريس، لورين، قادة موضوعات اللجنة الاستشارية الحكومية GAC. وشكرًا للجميع. سوف نجتمع مرة أخرى هنا تمام الساعة 15:00 بتوقيت كانكون، 20:00 بالتوقيت العالمي المنسق، من أجل اجتماعنا الثنائي مع مجلس الإدارة. لذا أرجو أن يكون سريعًا. شكرًا.

[نهاية التدوين النصي]