ICANN73 | منتدى المجتمع الافتراضي - الجلسة العامة: تطوير نقاش إساءة استخدام DNS
الثلاثاء 9 مارس/أذار 2022 – من الساعة 10:30 إلى الساعة 12:00 بالتوقيت الأطلسي القياسي

بريندا بريور: هل يمكننا البدء في التسجيل --

يجري التسجيل.

بريندا بريور: أهلًا وسهلًا ومرحبًا بكم في الجلسة العامة لـ ICANN73: تطوير نقاش إساءة استخدام DNS.

اسمي بريندا بريور وأنا مديرة المشاركة عن بُعد. يُرجى العلم بأن هذه الجلسة يجري تسجيلها وتتبع معايير السلوك المتوقعة في ICANN. لضمان شفافية المشاركة في نموذج أصحاب المصلحة المتعددين في ICANN، نطلب منكم تسجيل الدخول إلى جلسات Zoom باستخدام اسمكم الكامل. على سبيل المثال، الاسم الشخصي واسم العائلة أو اللقب. قد تتم إزالتكم من الجلسة إذا لم تقوموا بتسجيل الدخول باستخدام اسمكم الكامل.

تتضمن الترجمة الفورية لهذه الجلسة العربية والصينية والفرنسية والروسية والإسبانية. انقروا فوق زر "الترجمة الفورية" في شريط أدوات برنامج زووم Zoom لاختيار اللغة التي تفضلون الاستماع إليها.

خلال هذه الجلسة، ستُقرأ الأسئلة أو التعليقات المرسلة في الدردشة بصوت عالٍ فقط إذا وُضعت بالشكل المناسب كما أشرت في الدردشة. سوف أقرأ الأسئلة والتعليقات بصوت عالٍ خلال الوقت المحدد من قبل مشرف هذه الجلسة. وإذا أردتم الحديث خلال القسم المخصص لمناقشة المجتمع فيرجى رفع أيديكم بالضغط على زر رفع اليد في شريط أدوات برنامج زووم Zoom.

ملاحظة: ما يلي هو ما تم الحصول عليه من تدوين ما ورد في ملف صوتي 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 ينبغي ألا تُعامل كما لو كانت سجلات رسمية.

وقبل التحدث، يرجى منكم كتم صوت جميع الأجهزة والإشعارات. ويرجى التأكد من أنكم قد اخترتم لغة الاستماع المفضلة لديكم. ويُرجى التحدث بوضوح وبسرعة معقولة للسماح بالترجمة الدقيقة.

وبمجرد أن ينادي منسق الجلسة على اسمكم، يُرجى التكرم بإلغاء كتم صوت الميكروفون، ثم ذكر اسمكم للعلم والإحاطة. لعرض التدوين الآني للحوار، انقروا فوق زر التسمية التوضيحية المغلقة في شريط أدوات برنامج Zoom. فلنرحب الآن بمنسق الجلسة غرايم بونتون.

الرجاء البدء.

غرايم بونتون: شكرًا يا بريندا. صباح الخير أو مساء الخير للجميع. شكرًا لانضمامكم إلينا في جلسة اليوم بعنوان: تطوير نقاش إساءة استخدام DNS، التسجيلات الضارة وأسماء النطاقات المخترقة.
اسمي جرايم بونتون. وأنا المدير التنفيذي لمعهد إساءة استخدام DNS.

أولا، أعتذر لكم عن طول المقدمة التي سألقيها عليكم الآن. لدينا موضوع معقد، ومعنا مجموعة من أعضاء اللجنة المذهلين، لكن هناك قدرًا لا بأس به من الإعداد والتمهيد والذي نحتاج إلى وضعه قبل الدخول فعليا في الموضوع. ولذلك أرجو أن تصبروا قليلا.

سيعطينا مقدمنا الأول، ماسيج، مقدمة متماسكة عن جوهر الموضوع. لكني أريد التأكد أن الجميع هنا على نفس الصفحة أثناء إلقاء المقدمة.

وهذه محاولة مني في شرح ما نتحدث عنه اليوم في جملتين. بلغة بسيطة، تدور جلستنا اليوم حول استكشاف الاختلافات بين عمليات تخفيف أضرار النطاقات التي تم تسجيلها

عمدًا لإحداث ضرر والنطاقات التي تستخدمها مواقع الويب التي تم اختراقها أو التسلل إليها والتي تُستخدم أيضًا لإحداث أضرار. ففي إحدى الحالتين، يحاول شخص ما عمداً القيام بأشياء سيئة باستخدام اسم النطاق وفي الحالة الأخرى لا يفعل ذلك. وعلينا أن نفهم كيف يتم التعامل مع هذا التعقيد داخل نظامنا البيئي.

وقبل أن ندخل في - الجوهر، أريد أن أتطرق إلى بعض ما يتعلق بأهداف الجلسة ونطاقها وأن أعطيكم لمحة عامة عن الطريقة التي أعتقد أننا سنتبعها في هذه المحادثة.

بريندا، هل يمكنني الحصول على الشريحة الثانية، على ما أعتقد، من فضلك.

الأهداف العامة - إذن هذا ما سنحاول تحقيقه اليوم في مدة 90 دقيقة القصيرة التي لدينا. نريد أن نحاول تطوير فهم المجتمع لأهمية هذا التمييز بين التسجيلات الضارة والمواقع المخترقة. نريد أن نتحدث قليلاً عن كيفية عمل هذا التمييز وكونه مشكلة فنية في بعض النواحي، ولن نتعمق كثيرًا في ذلك.

ولكن نريد بعد ذلك التعمق في - وهذا هو جوهر هذه المحادثة. نريد تطوير فهم المجتمع لما يمكن القيام به في أي من سيناريوهات التسجيلات الخبيثة مقابل التسجيلات المخترقة والبحث في ذلك.

وأخيرًا، نريد التحدث بعد ذلك كله عن الأنشطة المحتملة، أي ماذا يمكننا أن نفعل حيال هذه المشكلة؟ ومن عليه تنفيذ ذلك؟ وما هو دور المجتمع.

فلننتقل إذن إلى مجال العمل. وهذا أمر مهم. لقد عملت في ICANN لفترة طويلة جدًا، وشاركت في الكثير من الجلسات العامة. وأعتقد أن هناك علاقة بين مدى تحديد نطاق النقاش في الموضوع ومقدار القيمة المضافة التي نحصل عليها في جلسات مثل هذه. ولذا أريد من الجميع هنا أن يلتزموا معي بنطاق ضيق للغاية في موضوعنا اليوم.

إذن، هناك بعض الافتراضات التي نفترضها لإجراء هذه المحادثة. وما أعنيه هنا هو أننا سنفترض أن السجل أو أمين السجل قد تلقى تقريرًا عن إساءة استخدام معينة. لكن كيفية توصله بهذا التقرير ليست مطروحة للنقاش اليوم. سنفترض أيضا أنه تم التحقق من الإساءة. أي أن هناك إساءة حقيقية تحدث. ولا نحتاج إلى مناقشة ما إذا كانت الإساءة موجودة أم لا. إذن، التحقق من الإساءة يوجد خارج نطاق مناقشتنا.

وسنركز بشكل أساسي اليوم على أمثلة البرامج الضارة والتصيد. قد لا تستوعب هذه الأمثلة تعريف إساءة استخدام DNS بالكامل. وقد تكون هذه البرامج المحور الذي يدور عليه تعريف معظم الناس لإساءة استخدام DNS، لكننا لسنا هنا لمناقشة هذا التعريف. دعوني أكن واضحا جدا. لن ننخرط في مناقشة تعريفية لما يدخل أو لا يدخل في إساءة استخدام DNS.

نحن هنا اليوم لفهم التمييز بين التسجيلات الضارة والتسجيلات المخترقة.

ولذلك سنقيد النقاش في هذه الجلسة بالافتراضات التي قدمتها لكم. وسنحاول جمع التعليقات والأسئلة التي تقع خارج النطاق لمعرفة ما إذا كان هناك مكان آخر للتطرق لتلك الأسئلة في المستقبل.

لكنني سأكون صارما في ضمان إبقاء نقاشنا في الموضوع. وأطلب من الجميع عند إرسالكم أسئلة إلى منصة الأسئلة والأجوبة أو عند مناقشتكم لما يقال أن تلتزموا بالموضوع، وآمل أن تتفهموا أن حرصي على هذا يصب في مصلحة الجميع.

الشريحة التالية، من فضلك.

إذن هذه خريطة للمحادثة التي سنجريها اليوم. إذن، لدينا تقرير عن إساءة استخدام DNS في أمين سجل / سجل ما. علينا أن نتحدث قليلاً عن "لماذا؟"، أي عن سبب وجوب التمييز هنا. هل هناك - هل ينبغي أن تكون هناك عملية عامة موحدة للتعامل مع جميع أنواع الأضرار؟ إذا لم نتفق مع هذه الفكرة، واحتجنا إلى التمييز هنا، فنحن بحاجة إلى التحدث قليلاً عن كيفية عمل هذا التمييز. وما هي سمات التسجيلات التي ستقودنا إلى اتخاذ هذا الاختيار؟

ثم لدينا تياران هنا. لدينا عملية يجب أن نتحدث عنها، وهي عملية تتعلق بأسماء النطاقات المسجلة بشكل ضار، أي أسماء النطاقات التي تشارك عمداً في الإضرار عبر الإنترنت. ولدينا عملية أخرى للمواقع المخترقة وما يجب أن نفعله حيال ذلك.

وأتوقع أن الجوهر الحقيقي لهذه المحادثة، أو أن الأجزاء الشائكة الحقيقية التي نحتاج إلى اكتشافها كمجتمع هو ما يتعلق بما يجب فعله في عملية المواقع المخترقة. لكننا سنغوص في هذين الموضوعين خلال جلستنا هذه.

ولدينا لجنة رائعة حاضرة معنا اليوم. سنبدأ بمقدمة من ماسيج، الأستاذ في جامعة غرينوبل - أو (نطقها بالفرنسية) إذا كنت فرنسيًا - الذي سيقدم لنا بعض البيانات وفهمًا لوضع الميدان. سيستغرق ذلك حوالي 15 دقيقة.

وبعد ذلك سننتقل مباشرة إلى حلقة النقاش. وفي لجنتنا اليوم بعض الأشخاص المميزين للغاية. شكراً جزيلاً لكم جميعاً على حضوركم. معنا لوري شولمان من IPC. ومعنا كريس لويس إيفانز من مجموعة عمل السلامة العامة في GAC؛ وآلان وودز من السجلات؛ وريغ ليفي من أمناء السجلات؛ ورود راسموسن من SSAC. ونحن بصدد البحث في هذه الموضوعات كما هي معروضة علينا هنا.

والنقاش مقسم إلى قسمين تقريبا. أولاً، سنلقي المقدمة، ثم سنتطرق قليلاً للبرامج الضارة ثم سنجري المزيد من المحادثات حول مواقع الويب المخترقة.
وسنخصص قدرا من الوقت في النهاية لأسئلة الحضور. ستكون لوحة الأسئلة والأجوبة مفتوحة لهذه المحادثة بأكملها، وأنا أشجعكم على استخدامها مع التحذير بأننا نحاول هنا التركيز على الموضوع المطروح اليوم.

فإذا لم تتم الإجابة على سؤالك، فاعلم أننا سنقوم بالاحتفاظ به للمناقشات المحتملة لاحقًا، ولكن، من فضلكم، لا تنزعجوا كثيرًا إذا لم تتم الإجابة عليه في سياق ما نناقشه هنا اليوم.

إذن، أعتقد أن هذا هو كل ما أردت مشاركته معكم في هذه المقدمة الطويلة نوعا ما، لكنني أعتقد أن لدينا بعض التوقعات، ولدينا بعض الأهداف الواضحة، وبعض المجالات الواضحة، وربما حان الوقت للبحث فيها.

وبهذا، أعتقد أنني مستعد لإعطاء الكلمة لماسيج الذي سيخبرنا بـ "ما يحدث اليوم" في الواقع، حول ما يتعلق بأسماء النطاقات الخبيثة والمخترقة.

إذن، تفضل يا ماسيج.

ماسيج كوركزينسكي: شكرًا لك يا غرايم على المقدمة.

مرحبًا بكم جميعًا. سأناقش اليوم بإيجاز مشكلة أسماء النطاقات المخترقة مقابل أسماء النطاقات المسجلة بشكل ضار. وسيعتمد نقاشي بشكل أساسي على مشروع COMAR، وهو مشروع بحث ممول من قبل AFNIC و SIDN، وهما مشغلان مسجلان لنطاقات .FR و.NL ويعتمد أيضا على الجزء الفني من دراسة إساءة استخدام DNS بتكليف من المفوضية الأوروبية.

الشريحة التالية من فضلك.

هنا في الجزء العلوي، يمكننا أن نرى عنوان URL تم وضعه في القائمة السوداء بواسطة Phish Tank، ويمكنك أدناه رؤية موقع ويب ضار، لقطة شاشة لموقع ويب ضار. والسؤال الذي نحاول الإجابة عنه اليوم هو: هل تم تسجيل اسم النطاق هذا بنية الإساءة. الشريحة التالية من فضلك.

للإجابة على هذا السؤال، نحتاج إلى التحقيق في هذه الحالة أكثر قليلاً. فعندما نزور اسم النطاق المسجل، يمكننا أن نرى أنه لا يوجد محتوى ذو معنى، وأيضًا، عند إلقاء نظرة على معلومات WHOIS، نرى أنه تم تسجيله قبل يومين فقط من إدراج عنوان URL الفعلي في القائمة السوداء.

الشريحة التالية من فضلك.

وهذا يوفر لنا دليلًا قويًا على أن اسم النطاق تم تسجيله بشكل ضار وتمت إساءة استخدامه لتقديم محتوى غير قانوني ومسيء وتصيد بيانات الاعتماد وانتهاك العلامات التجارية.

إذن ما هي نتائج ذلك؟ ما هو الوسيط الذي يجب أن يخفف من إساءة الاستخدام من الناحية الفنية؟ لذلك يجب أن يكون مشغل خدمة DNS -- على سبيل المثال، أمين السجل، وفي النهاية سجل TLD - وكذلك مزود الاستضافة. ولماذا يعتبر هذا مهما جدا؟ لأنه إذا قمنا فقط بتعليق اسم النطاق ولم نقم بتعليق الاستضافة الضارة، فقد يقوم المهاجم ببساطة بتسجيل اسم نطاق آخر ثم يوجهه إلى الاستضافة الضارة. من ناحية أخرى، إذا قمنا فقط بتعليق الاستضافة ولكن ليس بدون حظر اسم النطاق، فيمكن إعادة استخدام اسم النطاق من قبل المهاجم في هجمات أخرى، أي في حملات التصيد الاحتيالي الأخرى.

ولذلك فلزيادة الحواجز التي تحول دون إساءة الاستخدام وزيادة التكلفة الاقتصادية للمهاجمين، يجب أن يكون الاحتراز من جهة كل من DNS والاستضافة من منظور تقني.

الشريحة التالية من فضلك.

ودعونا نتحرّ حالة أخرى. هنا لدينا اسم نطاق آخر - آسف، عنوان URL آخر، عنوان URL ضار، تم إدراجه في القائمة السوداء، بواسطة مجموعة عمل مكافحة التصيد الاحتيالي إذا كنت أتذكر. يمكننا أدناه رؤية لقطة شاشة لصفحة الويب الضارة. إذن نفس السؤال هنا، هل اسم النطاق مسجل بشكل ضار؟

الشريحة التالية من فضلك.

إذن عندما نزور اسم النطاق المسجل، يوجد موقع ويب يحتوي على محتوى شرعي، ويتوافق المحتوى أيضًا مع اسم النطاق نفسه. وعندما نلقي نظرة على معلومات WHOIS، نجد أنه تم تسجيل اسم النطاق مرة أخرى في عام 2014، لذلك من المحتمل أن يكون اسم النطاق نفسه شرعيًا.

وكذلك، عندما نلقي نظرة على عنوان URL الضار، يمكننا أن نلاحظ أن wp-include، مما يشير إلى أن موقع الويب الفعلي قد تم اختراقه من خلال استغلال تثبيت Word Press الضعيف.

الشريحة التالية من فضلك.

ولذلك فإن اسم النطاق شرعي، ولكن تم اختراق موقع الويب وإساءة استخدامه لتقديم محتوى غير قانوني ومسيء، وتصيد بيانات الاعتماد، وانتهاك العلامات التجارية.

إذن ما هي آثار ذلك من منظور تقني؟

لذلك، بشكل عام، لا ينبغي أن يكون أمين السجل أو سجل TLD هو من يحظر اسم النطاق، لأن ذلك قد يتسبب في أضرار جانبية للمسجل وللعمل التجاري الذي يقف وراءه وكذلك للزائرين الشرعيين للموقع. لذلك يجب أن يكون الاحتراز على مستوى الاستضافة من خلال مزود الاستضافة أو المالك أو المسؤول عن موقع الويب. وهناك شيئان يجب القيام بهما. أولاً، تنظيف المحتوى الضار، وكذلك تصحيح الثغرات الأمنية وتثبيت Word Press.

والآن، من يجب أن يفعل ذلك؟ يجب أن يقوم بذلك إما موفر الاستضافة، إذا تمت إدارة الاستضافة مثلا على النظام الأساسي للاستضافة المشتركة حيث يتحكم النظام الأساسي للاستضافة في جميع البرامج، بما في ذلك البرامج الضعيفة، أو أن يقوم بذلك مسؤول الويب، إذا كنا نتعامل مع استضافة غير مُدارة ومسؤولها الذي يتحكم في البرامج الضعيفة في هذه الحالة.

الشريحة التالية من فضلك.

فكيف تتم إساءة استخدام النطاقات الشرعية؟ إذن، من خلال تحليلنا، وجدنا أنه تتم إساءة استخدام النطاقات بشكل أساسي على مستوى موقع الويب. فهناك برنامج ضعيف يتم استغلاله، على سبيل المثال، المحتوى والنظام المتقدم. يحدث ذلك أحيانًا على مستوى DNS. يمكن أن يكون أحد الأمثلة هنا هو تظليل النطاق حيث سيحاول المهاجمون أولاً التصيد الاحتيالي للحصول على بيانات اعتماد أمناء السجلات والمسجلين للوصول إلى لوحة التسجيل الخاصة بهم. وبمجرد تسجيل الدخول إلى لوحة التسجيل، يمكنهم إضافة، على سبيل المثال، نطاقات فرعية يمكن استخدامها في هجمات التصيد الاحتيالي مثلا.
الشريحة التالية من فضلك.

إذن ما هي الأساليب الحالية للتمييز بين أسماء النطاقات المشروعة ولكن المخترقة وأسماء النطاقات المسجلة بشكل ضار؟

هناك طريقتان. تعتمد الطريقة الأولى على الاستدلال، وغالبًا ما يستخدم هذا في تقارير الصناعة. وأحد المعايير الاستدلالية هو عمر اسم النطاق. أي، كما وضحت سابقًا، الوقت بين تسجيل الاسم ووضعه في القائمة السوداء؛ والتسجيل في الأنماط السائبة؛ وكذلك أنماط أسماء النطاقات المسجلة. على سبيل المثال، هجمات التصيد الاحتيالي أو أسماء العلامات التجارية أو الإصدارات التي في أسمائها أخطاء إملائية متعمدة وتشبه الخدمة المستهدفة، مثل PayPal.

والمجموعة الثانية من الطرق هي أساليب التعلم الآلي. وCOMAR مثال على ذلك، والذي تم تطويره في جامعة Grenoble Alps، بتمويل من AFNIC و SIDN، وهو نهج مؤتمت بالكامل، وفكرته هي جمع البيانات المتعلقة بالاستضافة إلى موقع الويب، وبنية عنوان URL، وتحديد QRs وما إلى ذلك، ثم نقوم باستخراج الميزات الـ 38. المشروع مؤتمت بالكامل على أساس النمذجة، وتصل دقته إلى 97%.

الشريحة التالية من فضلك.
إذن ما هي العلاقة بين نوع الإساءة وأسماء النطاقات المخترقة مقابل أسماء النطاقات المسجلة بشكل ضار؟ الشريحة التالية من فضلك.

ونعرض هنا توزيع أسماء النطاقات المخترقة باللون الأزرق والمسجلة بشكل ضار باللون الأحمر، حسب نوع إساءة الاستخدام. بالنسبة للبريد العشوائي والشبكة المشتراة التي يتم التحكم فيها، يحتاج المهاجمون إلى التحكم في DNS عموما. ومع ذلك، فإن هذا ليس هو الحال بالنسبة للتصيد الاحتيالي والأدوات التجارية. يمكن شن الهجمات باستخدام أسماء نطاقات ضارة أو مواقع ويب مخترقة، وكذلك عبر خدمات مجانية.

وهناك حوالي 25% من أسماء نطاقات التصيد الاحتيالي و 41% من أسماء نطاقات توزيع البرامج الضارة، المسجلة من قبل مستخدمين شرعيين ولكن من الراجح أنه تم اختراقها على مستوى موقع الويب.

الشريحة التالية من فضلك.

إذن ما هو الفرق حسب أنواع TLD المختلفة؟ لقد لاحظنا في النصف الثاني من عام 2021 أنه بالنسبة لنطاقات gTLD الجديدة، تم تصنيف 98% تقريبًا من النطاقات على أنها مسجلة بشكل ضار. إذا ألقينا نظرة على نطاقات ccTLD الخاصة بالاتحاد الأوروبي على اليسار، فإننا نرى أن 42% من النطاقات قد تم تصنيفها على أنها مواقع ويب مخترقة. وماذا سيكون - ما هي الأسباب المحتملة لذلك؟ نشك في أنه في الاتحاد الأوروبي ونطاقات ccTLD ستكون هناك تسجيلات أقل احتياطا، ومواقع ويب أكثر تميزًا وتقدم محتوى ذا مغزى، مما يعني أيضًا نشر برامج مختلفة يمكن أن تكون معرضة للخطر ويستغلها مجرمو الإنترنت على نطاق واسع.

الشريحة التالية من فضلك.

لذلك نرى هنا الفرق حسب نطاقات TLD المختلفة.

آسف، أعتقد أننا فقدنا الاتصال. لا أرى العرض.

غرايم بونتون: لقد ربط الاتصال من جديد ونحن نسمعك الآن يا ماسيج.

ماسيج كوركزينسكي: حسنًا. لكن لا أرى العرض.

غرايم بونتون: لا تزال الشريحة 13 معروضة حاليا.

ماسيج كوركزينسكي: نعم، حسنًا. سأنتقل إلى -- نسختي المحلية من العرض. حسنًا.

إذن، يمكننا هنا رؤية العدد الإجمالي لأسماء النطاقات ونطاقات إساءة الاستخدام لكل نطاقات TLD المختلفة وعدد المسجلين بشكل ضار وعدد الأشخاص المخترقين وعلى وجه الخصوص، في العمود الأخير، يمكننا رؤية النسبة المئوية للتسجيلات الخبيثة لجميع النطاقات التي تسيء استخدام نطاقات TLD معينة. الشريحة التالية من فضلك.

لذلك، بالنسبة لبعض نطاقات TLD، نرى النسبة المئوية لأسماء النطاقات المسجلة بشكل ضار تقريبًا 100%.

فقط لذكر أسماء نطاقات .TK و .ML كانت Freenom توفر النطاقات مجانًا لمستخدميها، وهذا باب خلفي جذاب للمخادعين إن صح التعبير.

الشريحة التالية من فضلك.

من ناحية أخرى، نرى أيضًا نطاقات TLD ذات. على سبيل المثال، .BR، وفيها 34% فقط من أسماء النطاقات المسجلة بشكل ضار. ويمكن أن يكون هذا نتيجة لعدة عوامل. أود أن ألفت انتباهكم إلى أن هذه النتائج يجب أن تؤخذ بحذر بسبب القيود التي تحد من فاعلية المصنفات وأيضًا بسبب قيود القائمة السوداء نفسها. قد لا يمثلون الفضاء السيبراني بأكمله.

ولم هذا؟ لأن بعض مزودي القائمة السوداء قد يركزون على أسماء النطاقات المسجلة بشكل ضار باستخدام هذا - عن طريق تحديد كلمات رئيسية معينة وما إلى ذلك.

وهناك أمر أريد ذكره هنا وهو أن ما نراه في القائمة السوداء قد يكون مختلفًا أيضًا عما تتلقاه سجلات TLD في مكاتب المساعدة الخاصة بها عندما يقومون بتحليل الشكاوى الواردة من ضحايا الهجمات، لأن هذه القوائم السوداء قد لا تمثل الواقع بالقدر الكافي.

وملاحظتي الأخيرة هي أننا نرى من وقت لآخر اختلافات كبيرة جدًا في نطاق TLD واحد، مثل .INFO أو .COM، من شهر إلى آخر. فماذا يمكن أن يكون سبب ذلك؟ قد يكون من الأسباب المحتملة أن أحد الموزعين، مثلا، يقدم خصومات كبيرة على أسماء النطاقات التي يستغلها المهاجمون. وسنرى، في هذه الحالة، زيادة في النسبة المئوية لأسماء النطاقات المسجلة بشكل ضار بالنسبة للعدد الإجمالي للنطاقات المسيئة. ونرى من وقت لآخر بعض نقاط الضعف التي يتم اكتشافها في أنظمة إدارة المحتوى مثلا، والتي تؤثر على مئات الآلاف من أسماء النطاقات. وهذه أيضًا فريسة سهلة بالنسبة للمهاجمين. وقد يستغلونها على نطاق واسع. وبعد مدة معينة، في هذه الحالة، سنرى انخفاضًا في النسبة المئوية لأسماء النطاقات المسجلة بشكل ضار بالنسبة لعدد النطاقات الإجمالي.

الشريحة التالية من فضلك.

شكرًا جزيلًا لكم على اهتمامكم. آمل أن تساعدكم هذه المقدمة على بدأ النقاش. شكرًا.

غرايم بونتون: شكرًا لك، ماسيج. لقد أجبت مسبقا على عدد من الأسئلة التي طُرحت أثناء تقديمك للعرض، وأنا أقدر ذلك حقًا.

ومع ذلك، فقد كانت هناك بعض الأسئلة الأخرى في الدردشة يا ماسيج: هل يمكننا القيام بذلك باستخدام التعلم الآلي؟ هل توجد خوارزميات للكشف؟ وما هي دقتها؟ ولا أعتقد أننا نريد التعمق كثيرًا في "كيفية" القيام بذلك، ولكن أعتقد أنه سيكون من المفيد أن تمنحنا ربما دقيقتين أو ثلاث دقائق حول السمات المختلفة لأسماء النطاقات نفسها، أو مواقع الويب، وكيف يمكن للأدوات محاولة القيام بذلك تلقائيًا، أو ما هي الأدوات المفيدة للبشر لمحاولة القيام بذلك إذا لم تتوفر لديهم هذه التكنولوجيا. هل يمكنك توضيح هذه الأمور؟

ماسيج كوركزينسكي: بالتأكيد. فيما يتعلق بالسؤال الأول، قمنا بتحليل أهمية الميزات في مصنف COMAR.

ومصنف COMAR، كما ذكر أثناء العرض، هو خوارزمية تعلم آلي بالكامل. والميزات المفيدة جدًا فيه هي ميزات تعتمد على المحتوى. لذلك، على سبيل المثال، إذا اكتشفنا على موقع الويب أن هناك الكثير من التقنيات المختلفة المستخدمة في بناء موقع ويب ما، فهذا مؤشر على تعرض موقع الويب للاختراق.

وإذا رأينا بعض الكلمات الرئيسية الجازمة مثل ""PayPal، ليس فقط الأسماء ذات العلامات التجارية، ولكن كلمات رئيسية محددة جدًا، مثل "التحقق"، فقد أجرينا أيضًا مثل هذا التحليل للكلمات الرئيسية. ويشير ذلك إلى أن موقع الويب قد تم تسجيله بشكل ضار.

وكما تعلمون، يمكن للمصنف العثور على بعض الأشياء مثل عدد التقنيات، وهو أمر أصعب بكثير على البشر.

من ناحية أخرى، إذا أردنا القيام بذلك يدويًا، فهناك طريقتان مثل ما رأيناه في الأمثلة، كالوقت بين التسجيل والوضع في القائمة السوداء. إذا كان قصيرًا حقًا، فهذا مؤشر قوي على وجود - على أن اسم النطاق نفسه مسجل بشكل ضار.

إذا لم نر أي محتوى ذا معنى في اسم النطاق المسجل أو موقع التصيد الفعلي، دعنا نقل، في اسم النطاق المسجل، فهذا مؤشر آخر على أن اسم النطاق مسجل بشكل ضار.

وهذان المثالان هما مثالان جيدان حيث يمكن للبشر وكذلك للتعلم الآلي أو نهج التعلم الآلي اكتشاف هذه الأشياء.

غرايم بونتون: هذا عظيم. شكرًا لك، ماسيج. إذن هناك الكثير من الأخذ والرد في الدردشة. لا يمكنني متابعة جميع التعليقات في الدردشة لأنها كثيرة جدًا. فإذا كان لديكم سؤال ترغبون في تلقي إجابة عنه، ويتعلق بالموضوع، فيرجى استخدام حجرة الأسئلة والأجوبة حتى نتمكن من محاولة الاحتفاظ به.

هناك عدد من الأسئلة حول "كيف" يتم هذا الاكتشاف. هناك أمران قد تنظر إليهما وهما أن DNSAI أصدر دليل "أفضل الممارسات" حول هذا الأمر مؤخرًا.

أنا متأكد من أن أحد أصدقائي يمكنه البحث عن رابطه ووضعه في الدردشة. من فضلكم، شكرًا.

وقد قمت أنا أيضًا بتقديم عرض تقديمي حول تصميم هذه الأنواع من الحلول يوم الاثنين كجزء من يوم التكنولوجيا، والذي أعتقد أنه يقدم إطارًا لكيفية القيام بذلك.

لكن أعتقد أن علينا الانتقال قليلاً من قضية "كيف." ومن الواضح أن هناك اهتمامًا كبيرًا بهذه التقنية أو الأساليب البشرية في اتخاذ هذه القرارات حول ما إذا كان التسجيل ضارًا أم لا. لكن أعتقد أننا بحاجة إلى الانتقال إلى "لماذا" ثم "ماذا."

وسيكون هذا هو سؤالي الأول للجنة. هذا الخطاب لكم أيتها اللجنة.

يوجد سؤال محوري هنا، وهو: هل علينا أن نفعل هذا أصلا؟ هل يعقل أن نقسم عمليات الاحتراز إلى أنواع مختلفة؟ هل نحن بحاجة للتمييز بين الخبيث أو المخترق أم لا؟ وهل ينبغي لنا اتباع نفس النهج في كل شيء، أي اتباع نهج إساءة استخدام عام؟ أم أنه يجب أن تكون لدينا عمليات منفصلة؟

إنني أشعر بالفضول هنا، وأريد أن أعرف ما إذا كان هناك أي شخص يختلف مع الفرضية التي انطلقنا منها. هل نتعامل مع جميع الإساءات على أنها نفس الشيء؟

فلنبدأ من هنا إذن، ولنر ما إذا كان هناك أي شخص في اللجنة يريد أن يعلق على هذا بسرعة.

سأختار منكم. من فضلك يا ريغ.

ريغ ليفي: بالتأكيد. نعم. أعتقد أنه من الضروري للغاية إجراء هذا التمييز. لدينا الكثير من العملاء الذين يستخدمون منشئي مواقع الويب التجارية الذين يحتاجون إلى تحديثات منتظمة. وإذا لم يجروا هذه التحديثات، فغالبًا ما يكونون عرضة للمساومة. ويتم التواصل مع المسجل لمناقشة حقيقة أنه يحتاج إلى القيام بشيء ما في اسم النطاق لم يكن قد فعله منذ عشر سنوات ولم يفكر فيه أصلا منذ حوالي خمس سنوات ومنذ أن طرح الموقع. وهم يستخدمون البريد الإلكتروني فقط ويفترضون أن انتقال الأشخاص إلى موقع الويب

والاطلاع على معلوماتهم ثم الاتصال بهم عملية مفروغ منها. وعلينا التأكد من عدم تأثر أعمالهم بسبب وجود اختراق في النطاق.

غرايم بونتون: شكرا ريغ.

لدي آلان ثم كريس ثم لوري. وأتوقع أننا لسنا بحاجة إلى التعمق في "لماذا." سوف ننظر في هذا الأمر. وبعد ذلك سننتقل إلى الخطوة التالية.

تفضل آلان.

آلان وودز: شكرًا جزيلاً. أنا آلان وودز للعلم والإحاطة.

إذن، أجل، أعتقد أنه من المهم أن نقوم بهذا التمييز. وأنا أعلم أن هذا هو السبب الذي تم اكتشافه خلال سنوات عديدة. ولكن هذا من وجهة نظرنا كمشغل سجل، فعندما نتخذ إجراءً ضد أحد النطاقات، ستكون هناك الكثير من الأضرار الجانبية. ونحن لا نريد إيذاء ضحية أخرى، وهو المسجل، في حالة وجود اختراق.

لذلك أعتقد أننا بحاجة إلى أن نكون واضحين للغاية فيما إذا كنا سنقوم بعمل ما، فيجب أن تكون لدينا فكرة عن الحالة وتقدير للاختلاف. كنت سأستخدم عبارة "فارق بسيط"، لكنه فرق كبير بين هذين النوعين المختلفين من الضحايا.

غرايم بونتون: نعم. شكرًا لك، ألان.

كريس.

كريس لويس-إيفانز: نعم، شكرًا يا غرايم. أنا كريس لويس-إيفانز، للسجل.

وأعبر عن اتفاقي معك هنا، فأنا أعتقد أنه يجب أن نتعامل مع الحالتين بشكل مختلف. وكما قال آلان من قبل، لدينا نوعان مختلفان من الأذى هنا. إذن، في نطاق مسجل بشكل ضار، هناك ضرر أساسي. وفي نطاق مخترق، لدينا ضرر أساسي ثم ضرر جانبي نتسبب فيه.

وإذا تعاملنا مع الحالتين بنفس الطريقة فسيكون لدينا أيضًا نوعان من الضحايا، الضحية الأساسية ثم أولئك الذين قد يتأثرون بالأضرار الجانبية. فعلينا حقًا أن نكون قادرين على معالجة حالتهما وتقديم المساعدة الكافية لكليهما.

غرايم بونتون: شكرًا لك، كريس.

تفضلي يا لوري.

لوري شولمان: نعم. كنت سأقول إن IPC توافق على أن هناك حاجة مطلقة للتمييز. من المهم التمييز بين النطاقات الضارة والمخترقة على الأقل في الواجهة الأمامية من حيث مدى سرعة الاستجابة لمشكلة معينة.

ولكن في الوقت نفسه، على الرغم من ذلك، لا أريد أن أضيع في مسألة التمييز بين الضحية الفعلية نظرًا لوجود المستخدم النهائي أو المستخدم النهائي الذي تم تصيده أو المستخدم النهائي الذي هو موضوع هدف هجوم برنامج ضار.

ولكن هناك أيضًا، لا سيما في حالة الشركات الصغيرة، احتمال تعرض هذا المالك المخترق للخطر، وتعرض سمعته للخطر. ولا أعتقد أنه يجب أن نفترض أن المسجل الذي يدير الأعمال - أو يدير أيًا منها - ليس بالضرورة شركة في حد ذاته، وقد لا يدير أي كيان خارج موقعه على الويب، وأيا كان، فإنه سيقبل أن يكون موقعه معطلا لفترة معينة من الوقت، إذا كان ذلك يحمي عملاءه أو سمعتهم.

غرايم بونتون: شكرًا لك، لوري.

إذن، ما أستنتجه هنا هو أنه، على الأقل داخل هذه اللجنة، لا يختلف أحد مع وجوب القيام بهذا التمييز. وهذا رائع.

لكن ذلك سيجعل عملنا أكثر تعقيدًا. والآن علينا أن نبدأ في البحث قليلًا عما يعنيه ذلك. بعد قولي هذا، لدينا عدد من الأسئلة في حجرة الأسئلة والأجوبة التي أعتقد أنه ربما يجب أن نحاول معالجتها قبل أن ننتقل إلى المواضيع التالية حتى تبقى الأسئلة ذات صلة مع ما نناقشه. سأحاول أن أختار بعضًا منها وأوجهها إلى أعضاء اللجنة. سنجرب ذلك.

كان هناك سؤال من غريغ شاتان أعتقد أنه موجه لماسيج. وكان سؤاله: كيف تتناسب إساءة الاستخدام على مستوى خادم البريد مع النهج الذي تقترحه؟

وأعتقد أن الإساءة على مستوى خادم البريد مثيرة للاهتمام. لا أعرف ما يكفي حول ذلك.

ماسيج، هل لديك أية أفكار حول كيفية معالجة ذلك؟

ماسيج كوركزينسكي: خادم البريد الإلكتروني؟

غرايم بونتون: أعتقد أن غريغ يسأل عن حالات التصيد الاحتيالي أو البرامج الضارة عبر البريد الإلكتروني.

ماسيج كوركزينسكي: هل من الممكن أن يطرح كاتب السؤال السؤالَ ببساطة؟

قد يكون من الأسهل حينئذ توضيح السؤال.

غرايم بونتون: أنا أحاول تجنب إعطاء الكلمة مباشرة هنا في هذه الجلسة.

يمكن أن يقوم غريغ بتفصيل سؤاله في الدردشة، وسنعود إليه لاحقا.

ماسيج كوركزينسكي: شكرًا.

غرايم بونتون: وانظروا ما إذا كان بإمكانه التوضيح.

ماسيج كوركزينسكي: شكرًا جزيلًا.

غرايم بونتون: ما الذي يمكننا الإجابة عليه قبل أن نستمر. أوه، هناك الكثير هنا. اصبروا معي بينما أحاول اختيار بعض الأشياء التي ستكون ذات صلة.

سؤال آخر لـ ماسيج موجه من سامانيه. وهي تتساءل عما إذا كانت طريقة ML والميزة المستخدمة في COMAR تتضمن أيضًا بعض الأساليب التجريبية التي أشرت إليها في الطريقة الأولى. وإذا كان كذلك، فهل لديك أمثلة؟

ماسيج كوركزينسكي: شكرًا لك على هذا السؤال. نعم، لقد قمنا بتضمين جميع الميزات المستخدمة في الاستدلال في تلك الأساليب تقريبًا باستثناء التسجيل الجماعي. هذه هي الميزة الوحيدة التي لم نقم بتضمينها. والسبب هو - هناك سببان. أحدها هو أننا - السبب الرئيسي هو أن طريقة COMAR يجب أن تميز المواقع الخبيثة مقابل المواقع المخترقة فقط بناءً على البيانات التي تم جمعها والمرتبطة بحالة واحدة محددة دون الحصول على - الحصول على معلومات من، على سبيل المثال، نطاقات أخرى مسجلة بشكل ضار.

ولكن بصرف النظر عن هذا، يتم تنفيذ جميع الاستدلالات في نظام COMAR الآلي بالكامل.

غرايم بونتون: شكرًا لك، ماسيج.

أعتقد أن هناك سؤالا آخر لك من مايكل بالاج حول رأيك في النسبة العالية لأسماء النطاقات المخترقة داخل نطاقات ccTLD الأوروبية وما إذا كان ذلك - أليس من المحتمل أن يُعزى ذلك إلى العدد المتزايد من نطاقات ccTLD التي تقوم بفحص الهوية؟

هل من الأسهل على الأفراد الضارين اختراق نطاق / موقع ويب بدلاً من تسجيل اسم نطاق ببيانات مسجّل احتيالي أو اصطناعي؟

ماسيج كوركزينسكي: إذا فهمت السؤال بشكل صحيح، فإنه كالتالي: لماذا نرى عددا أقل من مواقع الويب المسجلة بشكل ضار وعددا أكثر للاختراقات في نطاقات ccTLD الخاصة بالاتحاد الأوروبي. هل هذا صحيح؟

لقد حاولت مناقشة الإجابة قليلاً أثناء العرض. لكن يمكننا التكهن فقط لأننا لم نجر أي قياسات.

لكن أقول أنه لدينا، في نطاقات ccTLD للاتحاد الأوروبي، - كما ذكرنا سابقًا، عدد أقل من النطاقات المحجوزة، وليس هناك عدد كبير من النطاقات التخمينية. هناك مواقع ويب وراء أسماء النطاق. لذلك إذا كانت هناك مواقع ويب، فسيهتم بها مستخدموها أيضًا. لقد وضعوا - قاموا بنشر برامج مختلفة. ونظرًا لأننا نرى الكثير من البرامج المختلفة على موقع الويب، فقد يتم استغلال بعض البرامج - ببساطة.

وأعتقد أن الجزء الثاني من السؤال كان: لماذا نرى عددا أقل من أسماء النطاقات المسجلة بشكل ضار. هذا أيضا أمر تخميني بحت. ولكن هناك العديد من المبادرات في نطاقات ccTLD التي تمنع عمليات التسجيل الخبيثة. وأذكر فقط أن هناك نظاما، بالنسبة لـ ccTLD في الاتحاد الأوروبي، وهو نظام يشبه Premadoma يقوم باكتشاف النطاقات - أعني النطاقات التي تم تسجيلها بنية الإضرار منذ البداية. وهناك نطاقات ccTLD أخرى تحارب وتحاول منع تلك التسجيلات الضارة، مثل SIDN AFNIC، على سبيل المثال.

وهذا ما تبين لي من خلال خبرتي وأبحاثي وممارساتي التي أراها في نطاقات ccTLD. لكن لا يعني ذلك أن نطاقات ccTLD الأخرى، ومجموعات نطاقات ccTLD الأخرى لا تستخدم هذه الأساليب.

غرايم بونتون: شكرًا لك، ماسيج.

إذن، لدينا الكثير من الأسئلة والكثير من النقاش في الدردشة. سنبذل قصارى جهدنا في التعامل مع كل ذلك.

أعضاء اللجنة، إذا كنتم تريدون الإجابة على سؤال ما، إما مباشرة أو عن طريق الإجابة في حجرة الأسئلة والأجوبة، فلا تترددوا في القيام بذلك.

لكنني أعتقد أنه ربما ينبغي لنا الآن أن ننتقل قليلاً إلى الجانب الأيسر من هذا الرسم التخطيطي ونبدأ في الحديث عن شكل العملية المتوقع بالنسبة للتسجيلات الضارة والاعتبارات المأخوذة في ذلك. ومرة أخرى، حتى نحرص على أننا جميعًا على نفس الصفحة، فقد قررنا أنه يجب علينا التمييز بين الحالتين. وتحدثنا قليلاً عن دوافع اتخاذنا لهذا القرار. ولدينا بعض سمات اسم النطاق. قد يكون ML. وقد يقوم شخص ما بذلك. وعلينا الآن معرفة ما سنفعله.

وهكذا على مستوى السجل وأمين السجل، فليس هناك الكثير من الخيارات ولكن ربما علينا استكشافها قليلاً.

وقد ألجأ هذه المرة إلى رود. رود، إذا كانت لديك أفكار حول الإجراءات التي يجب على السجل أو أمين السجل القيام بها عندما يواجهون إساءة استخدام DNS ويعتقدون أن التسجيل تم بشكل ضار.

هل لديك أفكار حول هذا؟

رود راسموسين: نعم، شكرًا. معكم رود راسموسين.

إذن، بمجرد أن تحدد - حددت تبعا لأي منهجية تستخدمها - ولنضع المنهجية جانبا لأننا لا نركز عليها الآن. قلنا، حسنًا، تبين لي أن هذا تسجيل ضار، فماذا أفعل؟

ولديك - بصفتك سجلا أو أمين سجل، خيارات قليلة جدًا. ستكون لدينا نتيجة واحدة أساسا وهي إزالة النطاق نفسه من DNS العالمي.

وهناك عدة طرق يمكنك من خلالها فعل ذلك. يمكنك حذفه على الفور وتعلن فورا أنك ستقوم بإزالة هذا التسجيل. إذا كان لديك تسجيل ضار تم إجراؤه في الأيام القليلة الماضية، فلديك بالفعل - استفد من خيار الحصول على تعويض مالي مقابل ذلك. بمعنى آخر، قم باسترجاع أموالك. هناك ميزة لذلك، ولكن هناك عيبًا أيضا وهو أنه يمكن لمن سجل النطاق في البداية أن يسجله مرة أخرى إما باستخدام نفس أمين السجل أو في مكان آخر، وإعادة تنشيط مخططه، مهما كان، ومع أنك - في نفس الوقت الذي يقوم فيه شخص ما بالإجراءات الاحترازية ضد المحتوى الضار أينما كان، فمن الواضح أنه - كما تعلمون، هناك الكثير من المواقع المخترقة التي يمكنها أن تعيد الكرة مرة أخرى. فهذا له مزايا وعيوب.

يمكنك تعليق النطاق. بمعنى آخر، لا تحذفه، بل تضعه في حالة تعليق. سيؤدي ذلك إلى إزالته من DNS، وبعد ذلك، بغض النظر عن عمر هذا التسجيل، سيبقى في وضع معلق. وهذا أمر يتعين عليك بعد ذلك التصرف فيه بصفتك أمين السجل أو السجل أو كليهما.

ثم يمكنك - هناك إجراءات احترازية أخرى يمكنك اتخاذها. لسنوات عديدة، قدمت مجموعة عمل مكافحة التصيد الاحتيالي صفحة مقصودة لمواقع التصيد الاحتيالي، فيمكنك بالفعل إعادة توجيه - إذا كان هناك هجوم تصيد احتيالي، على سبيل المثال، فيمكنك إعادة التوجيه - يمكنك بالفعل تغيير DNS وتوجيه الزائر نحو تلك الصفحة المقصودة لفضح التصيد الاحتيالي. قام أشخاص آخرون بأمور مشابهة لهذا. وإذا تعلق الأمر بالبرامج الضارة وما يشبهها، فيمكنك إنشاء ما يسمى بالبالوعة وإنشاء القدرة على إبلاغ الضحايا بأن أجهزتهم قد تعرضت للاختراق. تم القيام بذلك بعدة طرق مختلفة إما بشكل مباشر من قبل مقدمي الخدمات، أو عن طريق شركات الأمن، أو عن طريق تطبيق القانون، وما إلى ذلك. إذن، يمكنك القيام بدور نشط في محاولة إخبار العديد من ضحايا البرامج الضارة بأن أجهزتهم مخترقة. ومن أجل القيام بذلك، قد تحتاج إلى نقل اسم النطاق إلى كيان آخر، إما من السجل - أمين السجل - من منظور المسجل، عفوا. فعلى سبيل المثال، استولى مكتب التحقيقات الفيدرالي على النطاقات ونقلها. وقد فعلت Microsoft هذا عدة مرات أيضًا.

يمكنك أيضًا - هناك - تستخدم السجل الأخير - سجل الخيار الأخير الذي تم إنشاؤه للتعامل مع البرامج الضارة ثم توفير تلك البيانات مرة أخرى بشكل تلقائي للضحايا. هناك العديد من الخيارات المختلفة، ولكن هذا يوجب مجهودات في التأكد من أن لديك عملية جاهزة وأوراقا قانونية معدة.

والأمر الأخير الذي أريد إضافته إلى هذا هو أنه، بمجرد أن تحدد أن لديك تسجيلًا ضارًا من نوع ما، فقد يكون من الجيد البحث ومعرفة ما إذا كانت هناك نطاقات أخرى مصطفة، أو مستخدمة من قبل، يستخدمها نفس المسجل أو نفس الحساب المسجل. وعند فحص هذا الحساب، فمن المهم حقًا - وأعتقد أن ريغ أو غيره قد يكونون قادرين على التحدث عن هذا الأمر أكثر قليلاً - من المهم فهم ما إذا كان هذا الحساب قد تم إنشاؤه من قبل الشخص المعني أم أنه قد تم اختراقه وتم القيام بذلك باسمه لأنه قد يكون ضحية للتصيد الاحتيالي أو لنوع من سرقة بيانات الاعتماد.

والأمر الآخر الذي يجب فعله هو البحث عن نمط لسلسلة من الحسابات التي ربما تم إنشاؤها تحت أسماء مستعارة مختلفة، وما إلى ذلك، للبحث عن إساءة عبر مجموعة واسعة من النطاقات وربما حسابات المسجل التي يمكن أن تؤدي إلى - تدعم عادةً حملة واسعة النطاق، لأن بعض هؤلاء المخادعين بارعون جدًا في إخفاء أنفسهم من المسجلين الدؤوبين الذين يحاولون إبعادهم عن أنظمتهم.

كانت هذه بعض الأفكار التي أردت عرضها عليكم.

غرايم بونتون: شكرًا يا رود. كان ذلك رائعًا. وهناك الكثير من الأفكار في مداخلتك.

ولتلخيص ذلك، فإن أمناء السجلات لديهم ثلاثة أو - وأمناء السجلات معنيون هنا أكثر من السجلات، ولكن يمكن أن تشارك السجلات في هذا أيضا - إذن، يمكنك الحذف، وهذا ليس خيارا جيدا، ويمكنك التعليق ويمكنك التنبيه أو إعادة التوجيه. وهناك أسباب للقيام بالخيارات الثلاثة كلها. وعليك بعد ذلك التحقق من الحساب، ومعرفة ما إذا كان هذا الحساب يناسب نمطًا منفصلاً. وأعتقد أن كل هذه مدخلات مفيدة جدًا للأشخاص الذين يقومون بالتعامل مع الإساءات.

أريد أن أعرف رأي ريغ وآلان من اللجنة في هذه الأمور. هل يستخدمون هذه الأساليب بشكل متكرر؟ وإذا كان الأمر كذلك، لماذا؟ ولم لا؟

وأثناء تفكيركم في هذا - تفضلي يا لوري.

لوري شولمان: شكرًا. لدي سؤال حول ما قاله رود حول النظر في أنماط الإساءة والبحث عن مجموعة أوسع - من الأمثلة. واليوم، مع القيود التي عندنا نتيجة لتشريعات الخصوصية والسياسات الحالية، هل البحث الآن محدود فقط داخل أمين سجل معين أو يمكن للسجلات النظر عبر نطاق واسع من أمناء السجلات حيث قد يكون من المنطقي للسجل القيام بذلك التحقيق بدلا من أمين السجل؟

غرايم بونتون: قد يكون كذلك. شكرًا لوري.

رود؟

رود راسموسين: نعم، دعني أرد على ذلك. نعم، على السؤالين (ضحك). إذن، لأمين السجل قدرة فريدة على رؤية معلومات العامة التي تم تسجيلها، ومن بينها معلومات الاتصال وغيرها، وهي معلومات قيمة، ولها قيمة كبيرة في عمليات التحقيق هذه، وأعني بذلك ما كان ماسيج يتحدث عنه سابقًا. ولديهم القدرة على معرفة مصدر عمليات الاشتراك، وبطاقات الائتمان المستخدمة، وجميع هذه الأمور. فداخليًا، لديهم الكثير من البيانات التي تمكنهم من النظر في هذه الأمور.

أما خارجيًا، فقد يكون للسجل فكرة جيدة عن احتمال وجود نمط، خاصةً إذا كان يدعم ما يسمى بخوارزمية إنشاء النطاق. ويتم استخدامها بواسطة البرامج الضارة حيث توجد مجموعة محددة مسبقًا من النطاقات التي سيتم تسجيلها من أجل توفير الأوامر والتحكم لعائلات البرامج الضارة. وإذا رأيت سلسلة منها عبر مسجلين مختلفين، فلتعلم أن هناك نمطا.

يمكنهم أيضًا النظر في أمور أخرى مثل استضافة DNS والطريقة التي يتم بها تكوين النطاق فعليا على الإنترنت نفسه. لذلك إذا ألقيت نظرة على طريقة إعدادها لخوادم DNS معينة أو خوادم أسماء أو عناوين IP لاستضافة عناوين IP في نهاية المطاف، فيمكنك - يمكنك في كثير من الأحيان اكتشاف مثل هذه الأشياء، أو معرفة أنها مشبوهة على الأقل. إنه أمر قد ترغب في النظر فيه بشكل أعمق وسؤال أمناء السجل عنه، وذلك للتحقق من هذه الحسابات ومعرفة ما إذا كانت شرعية.

غرايم بونتون: شكرًا يا رود.

لدي فكرة، لكريس. إذا كنت - وليس عليك الإجابة فورا - سأعطي الكلمة لريغ وآلان قبل أن أعود إليك، ولكن قبل أن ننتقل من هذا الموضوع، أريد أن أعرف ما إذا كان من منظور تطبيق القانون، وأعني ما يخص التسجيل الخبيث سواء كنت ستكتفي عموما بمجرد التعطيل أو ما إذا كان ذلك - بالنسبة للتسجيل الضار، غالبًا ما تشارك في عملية التحقيق حيث أنك تريد المزيد من المعلومات في هذه العملية.

ريغ وآلان، باختصار من فضلكما. ثم ربما كريس. وبعد ذلك أعتقد أننا سنحاول الانتقال إلى الجانب التوفيقي، وبعد ذلك سنتناول المزيد من الأسئلة والأجوبة.

ريغ.

ريغ ليفي: شكرًا لك، غرايم. معكم ريغ ليفي من Tucows. نحن أمناء سجل بالجملة، وطريقتنا في التعامل مع هذا ستكون مختلفة قليلاً عن أمين السجل الذي له علاقة مباشرة مع المسجلين.

نحن نعمل بشكل أساسي مع الموزعين، ونبحث عن أنماط تعتمد على البائعين. فعندما تبدأ الكثير من الإساءات في الظهور من بائع معين، فإننا نتواصل معهم ونقول، مهلا، نحن خبراء في التعامل مع إساءة استخدام DNS. كيف يمكننا مساعدتك؟ وعادة ما نحل المشكلات على أساس ذلك.

ومع ذلك، لدينا أيضًا موزع داخلي، وعندما نرى مجموعة من النطاقات المسجلة بشكل ضار تأتي من عنده، فإنه يمكننا اتخاذ إجراء مباشر ضد المسجل المعني طالما أنه طرف محدد.

كما ورد في الدردشة، لا يستخدم المحتالون عادة - أسماءهم أو نفس الأسماء لتسجيل مجموعة من النطاقات. لذا فإن البحث عن أنماط كهذه ليس مفيدًا دائمًا.

وأعتقد أن السؤال الأول كان: هل ننظر إلى وقت تسجيل النطاق من أجل اتخاذ قرار بشأن ما إذا كان النطاق ضارًا أم مُخترقًا؟ ونعم، نحن نفعل ذلك بالتأكيد. ولسوء الحظ، فإن الكثير من أنظمة الذكاء الاصطناعي، التي يتم ذكرها أيضًا في الدردشة، تفتقد بعض الأمور أو توفر - أو تحدد نطاقًا واسعًا جدًا لعمليات الإزالة. لذلك نحن بحاجة إلى إجراء الكثير من الفحص اليدوي لما يقدمه لنا الذكاء الاصطناعي.

ومن القصص المفضلة عندي قصة تتضمن خوارزمية إنشاء النطاق. تمكن أحد المخادعين الأغبياء من تسجيل نطاق باسم يطابق بالضبط سلسلة الأحرف العشوائية التي يستخدمها DGA، وكان هذا الاسم مطابقا للاختصار الطويل لاسم فريق كرة قدم نسائي صغير جدًا - نسيت أين كان بالضبط في أمريكا الوسطى. لذلك (يضحك) عملنا مع جهات إنفاذ القانون والسجل للسماح لهم بتسجيله بالفعل.

لكن، مرة أخرى، فهذا مثال على مثل هذه الخوارزميات الحاسوبية التي ستطرح شبكة واسعة جدًا. آسف.

غرايم بونتون: شكرا يا ريغ، كانت النكتة ماتعة.

آلان، ثم كريس. أرجو منكما الاختصار لنستمر. شكرًا.

آلان وودز: بالتأكيد. بسرعة كبيرة. إنه لأمر رائع أن تلاحق أمين السجل لأن هذه هي الطريقة التي يجب أن يسير بها السجل في هذه المحادثة بالذات. وهذا ما قاله ريغ، مجرد مستوى أعلى. عندما تتحدث إلى الموزعين أو تتحدث إلى المسجلين، فأنا أتحدث في المقام الأول إلى المسجل الخاص بي أولاً. وأعتقد أنه من المهم جدًا من وجهة نظر السجل، عندما أكون في هذا الموقف، نعم، سننظر في تلك المؤشرات، وستقوم منصة TDNS الخلفية الخاصة بي بعمل ذلك، ولكن الأمر يتعلق التصعيد القائم على الأدلة مع أمناء سجلي حتى يتمكنوا من إجراء محادثات أكثر استهدافًا مع المسجلين لديهم.

وأعتقد أننا في الوقت الحالي خرجنا نوعًا ما إلى مناقشة عملية الاكتشاف، والتي أريد الابتعاد عنها لأننا نتحدث عن الوسط هنا وكيف - ماذا نفعل وكيف نحدد التسوية. لذلك أعتقد أن هذا جانب مهم هنا.

وهناك أمر وحيد الذي أريد قوله، وأعتقد أنه مهم أيضًا من وجهة نظر السجل. وأردت فقط أن أرجع قليلاً لشيء قالته لوري سابقًا وهو أن الشركات الصغيرة ستفضل أو لا تمانع في حالة توقف أعمالها. أعتقد أن الكثير من الشركات الصغيرة ستختلف معك تمامًا في هذا الشأن. وأعتقد أننا بحاجة إلى أن نكون واضحين للغاية بشأن تناسب الأضرار. هل الضرر الذي يلحق بالمسجل أكبر من الذي يلحق المستخدم النهائي؟ وإذا تمكنا من العمل على أساس التناسب هذا بدلاً من الإدلاء ببيانات أكبر نوعًا ما أو بيانات أوسع، فأعتقد أن الأمر يتعلق بالتأكيد بالتناسب، وعلينا التحدث عنه هنا.

غرايم بونتون: شكرًا لك، ألان. وسيكون هذا بمثابة جسر نحو الموضوع التالي من مناقشتنا، وسأعود إلى موضوع موازنة الأضرار بعد لحظات وبعد أن نسمع من كريس.

كريس لويس-إيفانز: نعم، شكرا لك. أنا كريس لويس إيفانز، للتسجيل.

إذن، لنبق في موضوع النطاقات المسجلة بشكل ضار يا غرايم، والذي أعتقد أن سؤالك يندرج داخله، نعم، في نهاية الأمر، نحن نتحدث هنا عن البرامج الضارة والتصيد الاحتيالي، إذن، لا بد أن يكون هناك شكل من أشكال التحقيق. ولن يكون مفاجئًا لأي شخص أن المخترقين لا يسجلون نطاقًا واحدًا فقط.

لذا - سيكون النطاق قيد التحقيق، وأي عمل يمكننا القيام به مع السجلات أو أمناء السجلات أو مقدمي خدمات الاستضافة لتحديد المزيد من النطاقات، والتحول من رد فعل إلى عمل استباقي، سيؤدي دائمًا إلى التسبب في المزيد من الضحايا والمزيد من الأضرار. إذن، على أي حال، نعم، إن ما تتطلع سلطات إنفاذ القانون إلى القيام به دائما هو التبديل ومنع الضرر.

شكرًا.

غرايم بونتون: شكراً لك، كريس.

حسنًا. إذن لدينا حوالي 35 دقيقة متبقية، ونريد الحرص على معالجة مجموعة من هذه الأسئلة الموجودة في قائمة الانتظار، وهناك الكثير من النشاط في الدردشة. شكرًا جزيلاً

لكم جميعًا على هذه المشاركة الرائعة التي نراها. لكننا، على ما أعتقد، قمنا حتى الآن بالعمل السهل، وهو تحديد أننا نريد القيام بهذا التمييز. وتحدثنا قليلا عن كيفية ذلك. وتحدثنا عن بعض الأمور المهمة من حيث ما يجب القيام به في ظروف التسجيل الضار. والآن لدينا الجانب الآخر، وهو موضوع أكثر تعقيدًا وهو ما يضم مثالا على إساءة استخدام DNS، وأمثلتنا تقول إن البرامج الضارة والتصيد الاحتيالي توجد على موقع ويب مخترق. إذن فإن الموقع نفسه موقع بريء. قد يكون موقع شركة صغيرة، وقد تكون مدونة لشخص ما. هل هو كذلك؟ ربما لا يكون كذلك، وهذا هو النقاش الذي سنقوم به الآن.

ما هي العملية التي علينا القيام بها لمعرفة ما يجب فعله في هذه الظروف؟ ما هو ميزان الضرر الذي يستخدم عادة؟

ولذا ربما سأبدأ بسؤال قد يعتبر استفزازيا لريغ وآلان مرة أخرى، وهو: إذا قُرر أن موقع ويب تم اختراقه وأنه يتصيد أو يوزع برامج ضارة، فإنه متورط في إساءة استخدام DNS، هل هناك حالات ستقومون فيها بقطع اتصاله؟ ستقومون بتعليق النطاق، دعنا نقل، لموقع مخترق.

آلان؟

آلان وودز: شكرًا. يكاد يكون الأمر سحريا، وهو يتعلق بعدم تناسب الأذى. هذا سؤال مثير للاهتمام وأعتقد أننا نحتاج إلى أن نعي تماما، نحن السجل، بأن لدينا أداة كليلة للغاية، وتتمثل في إزالة كل شيء على الموقع المعني، وكل شيء في النطاق المعني، وأي رسائل بريد إلكتروني مرتبطة بهذا النطاق. وحتى يمكن للسجل أن يقول: هل تعلم؟ لم أحصل في هذه الحالة على أي رد من أمين السجل، ولم أتلق أي رد من المسجل، ولا يزال هناك ضرر كبير حاصل. نعم، أعني أن هناك دائمًا حالات قد نقوم فيها بالحذف. ولكن ذلك

حسب تناسب الأذى. هل نتحدث عن - آسف، سأتحدث بسرعة أقل ليتمكن المترجمون الفوريون من الترجمة. أنا أتحمس أحيانا.

نحن نتحدث، كما تعلمون، عن أشياء تضر بحياة الإنسان. نحن نتحدث عن أشياء مثل مواد الاعتداء الجنسي على الأطفال، وأمور أخرى استثنائية شديدة الخلافية ومثيرة للسخرية. ونحتاج إلى أن نكون واضحين جدًا في أن هدف السجل ينبغي أن يكون تجنب الحذف مهما أمكن، ولكن أن يكون لديه هذا الخيار عند الضرورة.

غرايم بونتون: شكرًا لك، آلان.

ريغ ليفي: لمتابعة --

غرايم بونتون: تفضل يا ريغ.

ريغ ليفي: متابعة للحديث، نحن نميل إلى استخدام التعليق كخيار أخير للنطاقات المخترقة أيضًا. ونتواصل مع الموزع والمسجل مباشرة ونقول، مرحبًا، لقد حدث كذا. هل يمكنكم إصلاح ذلك؟ وحسب استجابتهم أو عدم ردهم، قد نبدأ في إعادة تعيين السجلات المختلفة واحدًا تلو الآخر حتى نتمكن من إيقاف تشغيل البريد، يمكننا - إذا كان هذا هو المكان الذي يحدث فيه الاختراق. يمكننا إعادة تعيين خادم الأسماء إذا كان هذا هو المكان الذي حدث فيه الاختراق.

في بعض الأحيان، يدفع ذلك الأشخاص للرد والقول، لم أكن أدرك أن هذا البريد الإلكتروني الذي أرسلته كان شيئًا أحتاج إلى الرد عليه، ولكن هل يمكنكم وضع (غير

واضح) على الإنترنت ومن ثم يمكنني إصلاحه. وهو جزء آخر من هذه القضية، وهو أننا أحيانًا - نحتاج إلى السماح للنطاق بالعمل من أجل حل المشكلة حتى يتمكنوا من تسجيل الدخول إلى موقع الويب الخاص بهم وإصلاح الخلل.

لذا فإن تعليق النطاق سيؤدي إلى التخلص من الاستخدام الضار، لكنه لن يسمح بأي استخدام آخر ولن يسمح بالقيام بالإجراءات الاحترازية.

غرايم بونتون: شكرًا يا ريغ، وشكرًا يا آلان، على هذه المساهمة.

أريد أن أسأل لوري ورود وكريس مثلا، عما إذا كانت هناك معلومات تعتقدون أنه يجب تضمينها في اختبار توازن الأضرار الذي يشارك فيه المسجلون غالبًا والذي تعتقدون أنها قد تكون ناقصة أو يمكن أن يكون - يجب لفت انتباه هذه الأطراف إليها، وأعني ما يتعلق بما يجب فعله مع موقع ويب مخترق يشارك في إساءة استخدام DNS.

لوري شولمان: نعم، غرايم، سأقوم بالرد على هذا إذا سمحت أولا، بسبب ما يحدث في الدردشة. فقد أدليت ببيان في الدردشة وأدى ذلك إلى توسيع المحادثة. لكن هذا يعود إلى ما شرحه ريغ، والذي أتفق معه شخصيا، وهو أنه عندما تبحث عن نطاقات معرضة للخطر، فأنت لا تنظر دائما بالضرورة إلى مجموعة من الحقائق. وكانت هذه هي النقطة التي كنت أحاول توضيحها في الدردشة، لكن أعتقد أنه تم تفسيرها بشكل مبالغ فيه، أليس كذلك؟

عندما تنظر في أسماء النطاقات المخترقة، فأنت تنظر إلى مسار قرار مختلف تمامًا فيما يتعلق بما ستفعله، ومتى ستفعل ذلك وكيف ستفعل ذلك لأن الأمر هناك اشتراك - على الأرجح نمط (غير واضح)، موقع ويب مباشر يعمل، يقدم خدمة ما أو بعض المزايا

الأخرى التي ستختفي إذا أردنا تعليق النطاق. ويمكن أن يشمل ذلك دخل شخص ما. جيد جدا.

لكن النقطة التي أحاول توضيحها تعتمد - وهذا يعود إلى وجهة نظر رود - وإلى وجهة نظر آلان حول ما نتحدث عنه، كما تعلمون، فيما يتعلق بالتصيد الاحتيالي أو البرامج الضارة. هل تم اختراق الموقع وهو الآن يعرض مواد إباحية؟ وأنا لن أقول أي شيء - سأعود إلى الوراء وأقول المواد الإباحية للأطفال حتى لا نناقش شرعية المواد الإباحية الأخرى أصلا. كما تعلمون، القضايا الواضحة التي قررناها كمجتمع ليست حالات متطرفة. لذلك سنستخدم CSAM، لأنني رأيت هذا في ممارستي الخاصة حيث تم اختراق أحد المواقع، ثم بدأ الضحية يرى CSAM تعرض على موقعه. وكـ - ومرة أخرى، سأتكلم عن الشركات الصغيرة أكثر من الشركات الكبيرة، لأن الشركات الكبيرة لديها، مرة أخرى، أنماط قرار مختلفة في كيفية استجابتها لهذه الأمور. وقد تكون الشركات الصغيرة - قد يكون من مصلحة الشركات الصغيرة أن تقول، "لسنا بحاجة إلى CSAM مقترنة باسم النطاق هذا. نحن نقوم بتسويق اسم النطاق هذا. لدينا SCO على اسم النطاق هذا." يجب أن يتوقف هذا فورا. علينا أن نوقفه. علينا إعادة ضبطه. هذه وجهة نظري، وهي أنه لا يمكنك الحصول على مقاس واحد يناسب الجميع في أسماء النطاقات المخترقة. أعتقد أن أفضل ما يمكننا فعله - وأنا آسف، أنا آسفة للتحدث بسرعة كبيرة. سأتحدث بسرعة أقل. وأعتذر عن ذلك. إنها طباع الساحل الشرقي للولايات المتحدة تسري في عروقي. وأعتذر عن ذلك.

ما سأقوله ببطء أكثر هو أن هناك قرارات متشعبة ودقيقة يجب اتخاذها في التعامل مع النطاقات المخترقة. لا يمكننا أن نفترض ما يقبله أو لا يقبله مالك الشركة، وكما قلت يا آلان، إلا في الحالات المتطرفة.

لكن لا ينبغي أن نستبعد ذلك، وبالتأكيد لا ينبغي لنا أن نستبعد - وأنا أقدر ما تفعله Tucows، حيث إنها تتواصل مع بائعيها مما يتيح لهم معرفة ما يحدث.

أعتقد أن جزءًا كبيرًا من مشكلة الموازنة هو أن لدينا اعتبارًا للوقت اعتمادًا على مقدار الضرر الذي يحدث ومكان حدوثه، ثم نأخذ بعين الاعتبار المسجل الذي قد يقرر أنه من مصلحته الفضلى تعليق هذا النطاق في من أجل إعادة ضبطه حتى لا يضيع مجهودات التسويق والدعاية التي قاموا بها لشهر نطاقهم، وسأستخدم كلمة "مخففة"، وهو مصطلح مسجل. ولكن بهذا المعنى يمكن أن يتم تدمير كيان تجاري محترم بسبب بعض التنازلات التي نراها تحدث في ممارساتنا.

آمل أن تكون سرعة كلامي مناسبة.

غرايم بونتون: شكرًا لك يا لوري.

لدي كريس ثم آلان. وبعد ذلك سأطرح سؤالا على اللجنة.

كريس.

كريس لويس-إيفانز: نعم، شكرًا. أعتقد شخصيا، بالنسبة للنطاق الخبيث، أن السجل ومجموعات أصحاب المصلحة للمسجلين قد قاموا بعمل جيد حقًا في تقديم نصيحتنا المتعلقة بمعايير الإثبات التي يحتاجون الالتزام بها في الإخطار بإساءة الاستخدام.

ولم يتم إنجاز هذا العمل حقًا بالنسبة للنطاقات المخترقة. وأعتقد هنا أنه من أجل السماح للسجلات وأمناء السجلات بالتصرف، يجب أن تكون هناك بعض معايير الإثبات التي تحتاج إلى مزيد من التوضيح بالنسبة للنطاقات المخترقة.

كما تعلمون، إذا كنت مبلغا عن إساءة، هل يمكننا القول بأننا اتصلنا بشركة الاستضافة، وقمنا بالاتصال بأمين السجل، ولم يتم اتخاذ أي إجراء؟ مهما طال ذلك، فهو قيد المناقشة، ويعود هو أيضا إلى مستوى الأضرار التي تحدث.

كما تعلمون، بالتركيز على نطاقنا الضيق الذي نتحدث فيه عن البرامج الضارة، هناك جزء كبير من برامج الفدية التي يتم تداولها في الوقت الحالي. ويمكن أن تكون إصابة واحدة ببرامج الفدية السبب في نهاية عمل شخص ما وإخراج الكثير من الأشخاص من وظائفهم.

وحتى نكون قادرين على توضيح ذلك في معايير الإثبات المناسبة، قمنا مؤخرًا بعملية كبيرة ضد Amotech والتي كانت تسبب ضررًا جسيمًا للشركات والأفراد. ولنكون قادرين على توضيح ذلك وقول: لقد اتصلنا بمسجل النطاق، واتصلنا بموفر الاستضافة، ولم يحدث شيء، فنحن نتوجه إليكم الآن، يا أمين السجل أو يا أيها السجل، لتعليق النطاق لهذا السبب، مما يسمح حقًا ببدء عملية اتخاذ القرار.

ونحن نفهم أيضًا أنه قد يتعين بعد ذلك التحول إلى مناقشة، أليس كذلك؟ هذه شركة كبيرة متعددة الجنسيات وأنتم تطلبون منا تعليقها. سيكون تأثير ذلك هائلاً. في الواقع، تستهدف حملة التصيد الاحتيالي هذه بضعة أشخاص فقط. لديها سوق متخصص صغير جدًا، وسيكون التأثير هائلاً. من فضلك، هل يمكننا إعطاء المسجل 48 ساعة أخرى للرد، وسنلح أكثر في طلبنا.

لذلك أعتقد أن هناك محادثة كبيرة هنا مع النطاق المخترق. فهذا يقلل الضرر الذي يسببه النطاق المخترق بالنسبة للطرف الرئيسي وكذلك الأضرار الجانبية.

ونعم، يتطلب الأمر المزيد من الأدلة من المراسلين، ولكنه يتطلب أيضًا مشاركة أكبر قليلاً من الموجودين في السلسلة الذين يتخذون إجراءات ضد ذلك.

غرايم بونتون: شكرًا لك، كريس. هناك الكثير من المواضيع.

في هذا الجانب بالخصوص - ولذا أعتقد أنك محق تمامًا وأن هناك الكثير من العمل الذي يتعين القيام به في هذا المجال. كما أنه يتخطى بسرعة مسؤوليات أو خبرة السجلات والمسجلين في أماكن مثل شركات الاستضافة. وهذا سؤال أريد أن أعود إليه.

لكن، أولاً، تفضل يا آلان، من فضلك.

آلان وودز: في الواقع، بعد كل ما قاله كريس، أصبحت مداخلتي أقصر لأنني سأقول أمرا واحدا فقط - لقد فاجأت نفسي وكريس كذلك. كلانا يتكلم عن هذا، وهو SAC 115. وما نتحدث عنه حول قابلية التشغيل البيني، والتأكد من مشاركة المشغل المحدد في الوقت الصحيح، لضمان الاستجابة في الوقت المناسب، لأن هدفنا هنا هو الوقت المستغرق في هذا النطاق المحدد. وكلما دققنا في ذلك، قل الضرر الذي يمكن أن يحدث.

والذهاب إلى المزود الخطأ في الوقت الخطأ، يوسع ذلك نوعًا ما. وعلينا محاولة تجنب ذلك. وأنوه بمعهد إساءة استخدام DNS وجهوده المستقبلية في هذا الصدد. ونتطلع لهذا الأمر. أتطلع إلى أن أكون قادرًا على ربط مسار عملنا بمسار عملكم والقيام بكل هذه الأمور.

ولكن هناك أمرا واحدا أريد أن أشير إليه - وقد فاتني ذلك أيضًا - وهو أن بعض المسجلين، بالطبع، هم مسجلون لمنصات كبيرة ولديهم أيضًا إجراءات معقدة للغاية لمراقبة إساءة الاستخدام.

أعتقد أنك ذكرت ذلك يا كريس.

لن نوقف - فقط لاستخدام مثال واضح، التشويش الذي يتم إلقاءه - facebook.com. سأقول هذا. أنا لست .COM. نحن لا نحذف facebook.com بسبب حدوث سوء المعاملة على Facebook. سيكون ذلك سخيفا. لذلك أعتقد أننا بحاجة إلى أن نكون متوازنين للغاية في هذا النهج أيضًا.

غرايم بونتون: شكرًا لك، آلان.

كان هناك سؤال تم طرحه عدة مرات، وسأطرح هذا على آلان وريغ مرة أخرى لأنني أعتقد أن هذا يتطلب القليل من التفصيل للمجتمع، وهو: ما نوع العلاقة بينكم كمسجل أو أمين سجل مع الشركات المضيفة؟ لأن إحساسي هو أن هناك الكثير ممن يعتقدون أن هذه العلاقة قريبة جدًا. ولا أريد أن أتحدث نيابة عنكم، لكني أعتقد أن هناك العديد من الظروف التي لا تسمح بوجود علاقة قريبة.

وهكذا، كما تعلمون، نحن نتحدث عن مدى تعقيد هذه الأمور - وكريس يتحدث عن مسارات التصعيد بين المسجل والشركة المضيفة وبين أمين السجل والسجل، وهل هذه العلاقات واضحة؟ هل هناك معايير لهذه العملية؟ هل هذا مجرد ميدان يجب أن نقوم فيه ببعض الأعمال الإضافية؟ ريغ.

ريغ ليفي: شكرًا لك، غرايم.

ومرة أخرى، ستعتمد إجابتي على حقيقة أن Tucows هو في الأساس أمين سجل بالجملة.

لذلك قد تختلف الإجابة بالنسبة لأمناء السجلات الآخرين. ليس لدينا أي خدمات استضافة، ولهذا السبب لدينا استضافة دقيقة. ولدينا ما يقرب من 500 موقع في الشركة التابعة لنا. لذلك أقول أنه ليس لدينا استضافة أساسا.

[ضحك]

عادة ما يكون بائعونا أيضًا شركات مضيفة. لذلك، في كثير من الأحيان، يمكننا الوصول إلى البائع بالتجزئة والقول إن هناك حلا وسطا على هذا الموقع، ويمكنهم التطرق لذلك دون إشراك صاحب التسجيل. لذلك في حالة كون موزعنا هو شركة مضيفة، فلدينا تلك العلاقة، وهي علاقة وثيقة.

ومع ذلك، ليس هذا هو الحال الأنسب دائما. وهناك العديد من شركات الاستضافة. يعني الاستضافة خدمة تتطلب اسم نطاق. لكنها منفصلة تمامًا عن خدمة توفير تسجيل اسم النطاق.

وفي حالة عدم كون موزعنا هو الشركة المضيفة، فإن الأمر يصبح فوضويًا. ونحتاج إلى استخدام أداة DiG تمامًا مثل أي مستخدم آخر للإنترنت لمعرفة من هي الشركة المستضيفة ثم الاعتماد على أي معلومات يمكننا العثور عليها فقط بناءً على DiG للاتصال بالشركة المستضيفة.

غرايم بونتون: عذرًا، لقد فقدت السيطرة على مؤشر الفأرة.

شكرًا جزيلًا لك يا ريغ، الكلمة لآلان، بينما أصحح هذه الأخطاء. آلان.

آلان وودز: شكرًا. أعتذر لمترجمينا الفوريين مرة أخرى. أعرف أن الأيرلنديين يتكلمون بسرعة.

إن الأمر أكثر صعوبة من وجهة نظر السجل. ليس لدينا هذا الاتصال مع مزود الاستضافة. ربما نتوقع أن يتم هذا الاتصال قبل أن يعرض علينا المشكل. وربما نطلب أيضًا من أصدقائنا أمناء السجلات معرفة ما إذا كان بإمكانهم الاتصال أم لا، إذا كانوا أيضًا من مقدمي خدمة الاستضافة.

ما سأقوله، مع ذلك، هو أن هناك - وكلبي يشخر كثيرًا.

ما سأقوله هو أننا نتعامل معهم، أو مع ذلك، بقدر ما نستطيع في الخارج. لذلك من الواضح أن هناك العديد من المحادثات المختلفة. تقع إحدى هذه المحادثات ضمن سياق ICANN، ولكن هناك أمورا مثل الإنترنت والسلطة القضائية، والتي نحن أعضاء فيها، لأنه في تلك المناقشة، يوجد موفرو استضافة موجودون أيضًا على هذا الجدول لأنهم ليسوا ضمن سياق ICANN بشكل طبيعي. يمكننا إجراء تلك المحادثات التي تبني المزيد من الجسور مع مقدمي الاستضافة في أشياء مثل I&J.

أعتقد أن ما هو مهم بالنسبة لنا، مع ذلك، هو إعادة هذه المعلومات إلى مجتمع ICANN للإبلاغ عما نقوم به. أعتقد أن هذا شيء نقوم به أكثر. هذا ما حدث لأشياء مثل تعريف الإنترنت والسلطة القضائية ودخول ذلك إلى الأطراف المتعاقدة، وقد عملنا في ذلك.

فنحن نعمل مع مزودي الاستضافة قدر الإمكان ونخبر مجتمع ICANN بذلك، وهذا يعد أمرًا مهمًا بالنسبة لنا كذلك بصفتنا سجلات.

غرايم بونتون: شكرًا لك، آلان. أعتقد أن العديد من أمناء السجلات مضيفون ولكن ليسوا كلهم كذلك. لكن تحديد الاستضافة أو وجود علاقة مع المضيف، بالنظر إلى العدد الموجود حول العالم، ليس أمرا شائعًا. ولذا فهذا عائق حقيقي نحتاج إلى البدء في التفكير فيه، وهو كيفية تحسين عملية إعداد التقارير للمضيفين. ستكون لدينا المزيد من الأدوات التي نضعها تحت تصرفهم وسنكون مكانًا أكثر ملاءمة للعمل. ثم كيف نحدد مسارات التصعيد للسجلات وأمناء السجلات في حالات وجود مسجل غير مستجيب أو مضيف غير مستجيب؟ فالآن نحتاج إلى إعادة تقييم شكوى إساءة الاستخدام التي ظهرت.

لوري رفعت يدها، وقد بقيت لدينا حوالي 18 دقيقة. ولذا أعتقد أننا سننتقل بعد هذا لمحاولة معالجة بعض الأسئلة والأجوبة مباشرةً.
تفضلوي يا لوري رجاءً.

لوري شولمان: شكرًا. أردت أن أوضح بعض النقاط، وأتابع المحادثة بأفضل ما يمكنني.

لكنني أعتقد أنه من حيث الإبلاغ، وإمكانية التشغيل البيني، وخلق مساحات آمنة، فأعتقد أنه من الجدير أن ندرج في هذه المناقشة مقدار الاستثمار المعقول والذي يمكن أو ينبغي توقعه في هذه المساحة من حيث التقنيات الاحترازية. ويمكن أن يكون الأمر يتعلق بالعمل البشري هنا.

وحسب ريغ، فإن الذكاء الاصطناعي يلقي بشبكة واسعة جدًا. وكان EURid منفتحًا جدًا بشأن التحدث والقيام بعمل الذكاء الاصطناعي. ولا تزال بحاجة إلى جيش من البشر للتحقق من نتائج الذكاء الاصطناعي. لا أحد يأخذ النتائج كأمر مسلم به. وهذا أمر متوقع. نحن نتفهم وجود إنترنت أكثر أمانًا - على الأقل، تعلم دائرتي الانتخابية أن وجود إنترنت أكثر أمانًا قد يتطلب، في الواقع، الكثير من الاستثمار، وعلى هذا النحو، فقد

يتطلب في الواقع أسعارًا أعلى. وهل نريد التحدث عن ذلك؟ أعلم أن هذا يمثل مصدر قلق للمجتمع المدني بشكل خاص حيث من المهم أن يظل سعر أسماء النطاقات غير مكلف نسبيًا ومقبولًا لأي شخص يحتاج إلى نطاق ويريد بدء موقع شرعي.

لكن في الوقت نفسه، نعلم أن هناك سجلات معينة - ومسجلين يستثمرون أكثر. هل يؤتي هذا الاستثمار ثماره؟ وأعتقد أن هذا سؤال مهم يمكن للمجتمع أن يطرحه على نفسه.

غرايم بونتون: شكرًا لوري. في الواقع، أعتقد أنه من المحتمل أن يكون هذا مقدمة مناسبة للمجموعة التالية من الأسئلة المتعلقة ببعض ما يحدث في حجرة الأسئلة والأجوبة وفي الدردشة، وهي: ما هو دور هذا المجتمع؟ هل هناك دور لـ ICANN في محاولة معالجة بعض هذه التحديات التي اكتشفناها هنا اليوم. يمكن أن يكون هذا من أفضل الممارسات في التعامل مع التسجيلات الضارة. ما هو نطاق اختصاص ICANN فيما يتعلق بالمواقع المخترقة؟ ماذا يمكننا أن نفعل في ذلك الصدد؟ ما هي أماكن ذلك في المجتمع؟ هناك الكثير من الأشياء التي أريد التحدث عنها فيما يتعلق بـ DNSAI، لكني سأؤجل ذلك لوهلة.

أريد معرفة ما يريد أعضاء اللجنة أن يروه، وأية وجهة يرون أن على المجتمع اتباعها. لم أسمع من رود بعد. وأنا أشعر بالفضول حول ما إذا كانت لديك أفكار حول هذا. ريغ، لقد رفعت يدك.

تفضل رجاءً.

ريغ ليفي: شكرًا. أعتقد أن لفريق الامتثال في ICANN بند في العقود ينص على إنفاذ تلك العقود في الحالات التي لا يتم فيها اتخاذ إجراء ضد إساءة استخدام DNS. ويعني ذلك ضد المحتوى الذي يقع ضمن اختصاص ICANN والذي لا يتضمن، على سبيل المثال، محتوى غير قانوني، أو CSAM كما تمت مناقشته سابقًا، ولكن مع إساءة استخدام DNS. ويجب أن تستفيد ICANN بشكل أفضل من الاستخدام الفعلي لتلك البنود وإنفاذها.

غرايم بونتون: شكرا يا ريغ، الكلمة لرود ثم كريس.

رود راسموسين: إذن، قد أجبت على هذا السؤال. كان هناك سؤال مشابه في حجرة الأسئلة والأجوبة قمت بالإجابة عليه. أعتقد أن فاب طرحه.

إذن، تحدثت SSAC بالفعل عن هذا في SAC115 أي عن أن هناك دورًا لمنظمة ICANN ومجتمع ICANN الأوسع، بما في ذلك الأطراف المتعاقدة، وكل من يحضر مثل هذه الجلسات للمشاركة في النقاش. لكنه موضوع ذو نطاق أوسع، ونحن نركز عليه، كما تعلمون، ونستخدم عبارة "إساءة استخدام DNS". هذه مجموعة فرعية من جميع أشكال الإساءة على الإنترنت. وبعض التحديات التي تحدثنا عنها اليوم تدور حول مزودي الخدمة المناسبين للمشاركة في الاحتراز مهما كانت الأضرار، سواء كان الأمر يتعلق باختراق أو بتسجيل ضار، فهذه محادثة رائعة في هذا الموضوع، ولكن هناك أيضًا - فكر في معايير الإثبات، إلى متى - أو التوقعات حول الاعتراف بالإساءة المبلغ عنها والتخفيف من حدتها، وما هي أنواع الإجراءات التي يمكن أن تكون مقبولة هنا. هناك مجموعة كاملة من الموضوعات واسعة النطاق.

نحن نشهد تحركًا نحو ذلك. لدينا، كما تعلمون، مبادرات رائعة مثل النطاق - إساءة استخدام النطاق - معهد إساءة استخدام DNS وبعض الأعمال التي تقوم بها I&J، الإنترنت والسلطة القضائية. هناك الكثير من الجهد المبذول لإنشاء قائمة من المعايير، وأفضل الممارسات، وما إلى ذلك، ولكننا لم نتم ذلك بعد، ولدينا طريق طويل علينا قطعه في محاولة إنشاء - نظام بيئي يمكن فيه للناس أن يتوقعوا توقعات حول العملية وحول التناسب وكذلك العناصر الأخرى التي يحتاجونها لإنشاء استجابة ونظام وقائي أفضل ضد جميع أنواع الإساءة.

لذلك فمن المهم، على ما أعتقد، وبصفتنا مجتمع ICANN، أن نكون على نفس الصفحة قدر الإمكان، وننخرط بعد ذلك مع مجتمع الإنترنت الأوسع أيضًا وندرس كيفية التعامل مع هذه المشكلات، لأننا إذا حاولنا جميعًا حل الجزء الخاص بنا من اللغز فقط، فسنحصل على مجموعة من الأنظمة المختلفة. ولكن هناك الكثير من الأعمال الهادفة الجارية حاليا، وقد يكون لـ ICANN دور في تعزيز المحادثات نظرًا لأن لديها قدرا كافيا من الموارد، ولها باع أطول من الكثير من الجهود الأخرى، سواء كانت في ميدان الاستضافة أو البريد الإلكتروني، أو غير ذلك.
ولذلك فإني أشجع الناس بشدة على الاطلاع على SAC115 والمشاركة في بعض المحادثات التي ستكون محادثات فعالة واستباقية والتفكير - عالميًا في كيفية التعامل مع هذه المشكلات وإنشاء أطر كهذه، فنحن نحتاجها لتحديد التوقعات ومتابعتها.

شكرًا.

غرايم بونتون: شكرًا يا رود.

أعتقد أنني رأيت أحدهم يضع رابطًا إلى SAC115 في الدردشة، لكنني سأتأكد من قيام شخص ما بذلك مرة أخرى.

كريس ثم آلان.

كريس لويس-إيفانز: نعم، شكرًا. كريس لويس إيفانز للتسجيل مرة أخرى.

أتفق مع كل ما قاله رود، لكن أعتقد أنني كنت أنوي التعبير عن اتفاقي مع ريتش حول الامتثال في بداية حديثي. لكنني أعتقد، كما تعلمون، أننا (غير واضح) بشكل كبير حول كيفية التعامل مع إساءة استخدام DNS، وهذه المحادثة جزء من ذلك. لا أعتقد أن لدينا عملية مناسبة للتعامل مع النطاقات المخترقة والتي تعد جزءًا مهما من هذه المناقشة. إن وجود حد أدنى لما يُتوقع القيام به وتوثيق ذلك يسمح للعملاء بقياس الاستجابات، وأعتقد أن هذا سيكون مفيدا للغاية. و علينا بعد ذلك أيضًا تعميم هذه المعايير على جميع أمناء السجلات والسجلات حتى يعرفوا ما هو مطلوب منهم، وأعتقد أن هذا أمر أساسي حقًا. وأن نقدم لهم المواد التعليمية كذلك. كما تعلمون، هناك أنواع مختلفة كثيرة من السجلات وأمناء السجلات، و كما قيل، أعتقد أن معرفة أفضل الممارسات في كيفية التعامل مع هذه الحالات أمر أساسي حقًا بالإضافة إلى ما قلته.

وهناك الكثير مما يمكن لـ ICANN القيام به لنشر ذلك عبر ميادينها المختلفة. وكما قال رود، - في تعليقه، القيام ببعض التواصل في مناطق أخرى. وكما لاحظتم، فقد أشرنا كثيرا إلى شركات الاستضافة ومقدمي الخدمات خلال هذه الجلسة، وهم جزء رئيسي حقا، ولهم دور كبير في التعامل مع ما يتعلق بـ DNS في مثل هذه الحالات.

شكرًا.

غرايم بونتون: شكراً لك، كريس.

آلان، باختصار، وبعد ذلك سنحاول الإجابة على سؤال أو سؤالين قبل إجراء ملخص موجز.

آلان وودز: ممتاز. باختصار شديد. بالمناسبة، لقد بدأت المجموعة الفرعية لإساءة استخدام DNS الخاصة بمجموعة أصحاب المصلحة في السجل بالفعل، كجزء من هذه العملية بأكملها، وحتى قبل أن نقترح تنظيم هذه الجلسة العامة، عمليةً لمحاولة وضع ورقة بحثية، أو محاولة الشروع في ذلك على الأقل. ومن الواضح أن غرايم يشارك في ذلك. إنه القائد غير الرسمي حاليا، وأعتقد أننا سندعو أشخاصًا من SSAC أيضًا لمساعدتنا. ونحن نضم رود وجيف بيدسر أيضا على ما أعتقد، حتى نتمكن من إجراء هذه المحادثة القوية حول الحالات الخبيثة مقابل المخترقة؛ للقيام بالضبط بما قاله كريس للتو، أي محاولة وضع الأساس.

فقد كانت هذه محادثة افتتاحية. كانت جلستنا هذه بمثابة إقرار بأن هناك مشكلة، كما نعلم، تتعلق بانتهاك DNS ونحن نعمل على حلها، ولكننا نحتاج أيضًا إلى العمل على الفروق الدقيقة والاختلافات الموجودة في هذا الموضوع لمساعدتنا في التعامل معه بشكل فعال.

لذلك أدعوكم لمتابعة هذا الموضوع عن كثب، وآمل أن تكون لدينا قريبا نتائج في ذلك ويكون ذلك بداية قوية وجيدة جدًا.

غرايم بونتون: شكرًا لك، آلان. إذن الورقة التي نعدها هي TPH حول هذا الموضوع. أعتقد أننا نهدف إلى إنهائها من الآن وحتى الاجتماع في لاهاي، ICANN74 في يونيو. أعتقد

أن إتمامها سيكون أقرب إلى شهر يونيو من الآن، لكننا سنحرص على تعميمها وتوزيعها على المجتمع.

طرح فاب سؤالاً منذ وقت طويل في الدردشة حول هذا الموضوع تقريبا. فماذا يمكن أن يفعل المجتمع؟ هل هناك تغييرات على RAA يمكن إضفاؤها بإضافة بعض أفضل الممارسات أو ما يتعلق بالمشكلات التي نتحدث عنها اليوم؟ وهذا محتمل. أظن أن هذا خيار مطروح.

وقد تلقيت رسالة من معهد إساءة استخدام DNS بالأمس في تواصل من فريق DNSO الصغير معي حول مشكلات إساءة استخدام DNS يطرح مثل هذا السؤال. ولقد فكرت في هذا شخصيا لفترة، وأعتقد أن دور المجتمع هنا هو أخذ أجزاء صغيرة جدًا من هذه المشاكل الكبيرة. لقد تحدثنا كثيرًا عن تعقيد هذا النظام البيئي، خاصةً عندما تكون الإساءة في أسماء النطاقات المخترقة. وأعتقد أننا نريد أن نبدأ بالقضايا السهلة المتعلقة بالتسجيلات الضارة حيث تكون العواقب أقل عندما نحكم عليها بشكل خاطئ ويقل فيها عدد الضحايا المتورطين.

ولذا أعتقد أنه يمكننا البدء في التفكير في العمل الذي يناسب المجتمع فيما يخص التسجيلات الضارة. وأعتقد أن هذا يتناسب أيضًا مع اللوائح الداخلية لـ ICANN إلى حد ما. وهذا هو اقتراحي، وآمل أن يجيب هذا على سؤال فاب في الدردشة.

دعونا نر ما إذا - لدينا سبع دقائق أخرى. أريد أن أعطي الناس فرصة في حال كانت لديهم أفكار ختامية أو إذا كان هناك سؤال في حجرة الأسئلة والأجوبة يرغب أي شخص في الإجابة عليه مباشرة.

رفع ريغ يده. تفضل يا ريغ رجاءً.

ريغ ليفي: شكرًا لك، غرايم. أردت تسليط الضوء على شيء قالته آشلي في الدردشة؛ وهو أن مجموعة أصحاب المصلحة للمسجلين تعمل حاليًا على إعداد أداة يمكنك وضع اسم نطاق فيها، فتقوم بنشر معلومات حول هوية الشركة المستضيفة وكيفية الاتصال بهم.

فيرجى الانتباه لذلك. وقد قمنا بعرضها لأول مرة في مجموعة أصحاب مصلحة أمناء السجل في وقت سابق من هذا الأسبوع، لكننا نأمل أن تتوفر روابط مباشرة للجميع قريبًا.

غرايم بونتون: شكرا لك يا ريغ.

وأعتقد أن هذا أمر مهم، وهناك عمل مشابه يعده معهد إساءة استخدام DNS أيضًا سيكون أداة مركزية للإبلاغ عن إساءة الاستخدام. من الواضح تمامًا أن هذه العمليات لتحديد جميع المكونات في النظام البيئي، ومن هم، وكيفية الاتصال بهم، وما هي معايير الاتصال بهم، فكل هذا فوضوي جدًا في الوقت الحالي. ويمكننا القيام بعمل أفضل جماعيا، كما تعلمون، نشد أزر بعضنا البعض في مثل هذه العمليات وحل مشكلة الاتصال وجعل ذلك أسهل قليلاً. وأنا أعمل على بعض الأمور المشابهة حاليا. هذا ليس المكان المناسب للحديث عنها، لكنني سأشارككم أخبار ذلك لاحقًا.

لنر ما إذا كان بإمكاننا الإجابة عن سؤال أو سؤالين بسرعة هنا. مرة أخرى، نعتذر عن عدم استيعاب جميع الأسئلة التي تلقيناها.

أثناء قراءتي لقائمة الانتظار هذه، سأرى مَن من اللوحة يريد إعطاء أفكار موجزة حول هذا السؤال - أو هذا الموضوع الذي ناقشناه اليوم.

أرى لوري. تفضل رجاءً.

لوري شولمان: بالتأكيد. شكرًا.

أصبحت الدردشة سريعة جدًا ولا يمكنني متابعتها بعد الآن. لكني أريد أن أقول إنني أعتقد أن هذه اللجنة جاءت في الوقت المناسب ونحن بحاجة ماسة إليها. وأريد أن أشكر المنظمين على دعوة IPC وأشكرهم شخصيا لأنهم سلطوا بذلك الضوء على القضايا الصعبة.

لا أعتقد أن أي شخص يرى أن هذه قضايا سهلة. فهذا ليس موضوعا سهلا. لا أعتقد أن هناك من يقول أنه يجب علينا أن نتخذ قرارات متسرعة. لكنني أعتقد أنه، على الأقل من وجهة نظري، لا ينبغي لنا اتخاذ قرارات متسرعة - خاصة مع أسماء النطاقات المخترقة. يواجه المجتمع ما واجهه وعرفه ممارسو العلامات التجارية ومتخصصو إنفاذ القانون والأمن السيبراني منذ سنوات، وهو أن كل حالة من حالات الإساءة يمكن أن يكون لها نمط حقائق خاص بها. قد يكون لكل حالة إساءة علاج أفضل أو أسوأ. سيتم النظر في كل حالة من حالات الإساءة ضمن مجموعة الحقائق الخاصة بها.

لذلك مع كل ما يقال، من الواضح لي أنه يتحتم علينا كمجتمع وضع المعايير. وأعتقد أن المشاريع مثل I&J والأوراق مثل SSAC115 والعمل الذي تقوم به يا غرايم، يساعد حقًا في وضع تلك المعايير.

ولكن أين الجزء التالي من هذا؟ وأعتقد أنه من المناسب القول كيف تعمل المعايير الموضوعة خارج المجتمع، وكيف تعمل داخل ICANN أيضًا؟ ووضع اقتراح بعيد التفكير كهذا في الدردشة، والذي تمت مناقشته في دائرتي الانتخابية، وهو أنه عندما كانت لدينا مشكلة السيبرانية - آسف، حدث السطو الإلكتروني منذ 20 عامًا، لم يكن هناك نظام قضائي موضوع أو مقرر للمساعدة في هذه الحالات. ووجدنا ما يكفي من

القواسم المشتركة التي طورنا UDRP وفقها، والتي عملت بشكل جيد للغاية لمدة 20 عامًا.

هل حان الوقت للتفكير في عملية من نوع UDRP للنطاقات المخترقة؟ وسأتوقف هنا، لكنني أعتقد أنه سؤال للمستقبل، لأنه عندما نتحدث عن الحلول والمعايير، فإن هذا الأمر يستحق النظر.

غرايم بونتون: شكرًا لك، لوري. نقدر تلك المدخلات. وأيضًا استخدام كلمة المستقبل أمر مذهل.

أريد أن أجيب بإيجاز، قبل أن أنتقل إلى آلان، على سؤال من جريفين في الدردشة، أعتقد أننا تطرقنا إلى جزء منه بالفعل وهو عمل - داخل المجتمع، ولكن أيضًا كشخص يدير معهدًا مخصصًا في هذا الموضوع، ولوجود العديد من المختصين، فبالنسبة لي - من الواضح جدًا أن مشكلات إساءة الاستخدام تخرج من نطاق اختصاص ICANN بسرعة كبيرة حيث أننا نحتاج إلى التعامل مع المضيفين. ولذا لدينا العديد من المنظمات مثل Global Cyber Alliance و I&J و DNS Abuse Institute و topDNS من eco والتي تعمل بطرق مماثلة وتعمل على حل مشكلات مماثلة. وما يتعين علينا القيام به هو أن نكتشف طريقة نعمل بها معا. أي بشكل جماعي، وأعتقد أننا ندعم نموذج أصحاب المصلحة المتعددين و ICANN ونرى حقًا، كما تعلمون، الأهمية الواضحة لهذا العمل.

لكننا نحتاج أيضًا إلى معرفة أن هناك مكانًا للمنظمات المجاورة يمكن أن يمتد إلى ما وراء تلك الحدود والانخراط مع المجتمع الأوسع بطريقة ربما لا تكون مناسبة لـ ICANN أو، كما تعلمون، القواعد داخل نظام ICANN.

وبذلك سنكون قادرين على أن نبين للمصالح الخارجية، سواء كانت المنظمين في جميع أنحاء العالم أو غيرهم، ولـ ICANN داخل المجتمع، أن هناك مكانًا للعمل داخل المجتمع يولد المتطلبات التعاقدية و PDPs وأشياء من هذا القبيل، ولكن أيضًا صناعة تطوير أفضل الممارسات، للوصول إلى الأمور لاتي لها علاقة بهذا مثل الاستضافة، وموفري البريد الإلكتروني، ومثلها من أجزاء المجتمع، بحيث يمكن لكل منها التعاون والعمل معًا. وعلينا فقط أن نحسن طريقة قيامنا بذلك، لأن هذا سيفيد الجميع ويحل مجموعة من هذه المشكلات.

لدينا دقيقة واحدة متبقية. يبدو أن الكلمة الأخيرة ستكون لك يا آلان.

آلان وودز: أريد فقط أن أكرر ما قاله غرايم. وأعتقد أنه من المهم -- لا أختلف مع لوري. في الحقيقة، أنا أتفق كثيرًا مع ما قالته. أعتقد أننا نحتاج فقط للتأكد من أن UDRP هو اسم نطاق إلى حد كبير - كان يعالج مشكلة اسم النطاق إلى حد كبير. ما نتناوله هنا هو ما يقوله غرايم حرفيًا، وهو أوسع بكثير من مجرد السجلات وأمناء السجلات. نحن نتحدث عن موفري الاستضافة، وهذا الجانب من سياق ICANN. لذا، هناك شيء أوسع من ICANN، ولكن علينا القيام بدورنا والتعاون مع الأجزاء المكونة لـ ICANN، لمحاولة التوصل إلى نتيجة بشأن هذا الأمر. وأعتقد أن هذه هي الطريقة التي نمضي بها قدما في الوقت الحالي، وهي محاولة فهم هذه المنطقة القابلة للتشغيل البيني. نحن بحاجة إلى دعم وتفهم الجميع. ونحن نتحسن في ذلك. أعتقد أننا نتحسن في ذلك. ويجب أن نستمر في التحسن.

غرايم بونتون: شكرًا لك، ألان.

إننا على رأس الساعة. شكرًا جزيلًا لأعضاء اللجنة. وأريد أن أشكركم جميعا على بذل وقتكم في هذا. شكرًا على هذا العرض التقديمي الرائع يا ماسيج. أيها الجمهور، لقد أحسنتم اليوم في التزامكم بالموضوع وتقديم مدخلات أكثر بكثير مما كان يمكننا أن نتطرق إليه. وأعتذر لكم على ذلك. سنحاول الاحتفاظ ببعض منها ونرى ما إذا كانت هناك طريقة لدمج ذلك في جلسة أخرى أو بعض الأعمال الأخرى.

وبهذا، أعتقد أنه يمكننا إنهاء جلستنا هنا اليوم. وأشكركم مجددا على المشاركة الرائعة. لقد كانت قيمة فعلا.

[نهاية النص]