AR

ICANN83 | منتدى السياسات – ccNSO: DASC عمليات الاحتيال عبر الإنترنت والجرائم المالية
الأربعاء، 11 يونيو/حزيران 2025 – 13:45 إلى 15:00 بتوقيت وسط أوروبا الصيفي

كلوديا رويز

مرحبًا بكم في جلسة عمليات الاحتيال عبر الإنترنت والجرائم المالية من اللجنة الدائمة المعنية بانتهاك نظام اسم النطاق DASC التابعة لمنظمة دعم أسماء النطاقات لرمز البلد ccNSO. اسمي كلوديا رويز وأنا، إلى جانب زملائي، يوك وجولي، مديري المشاركة عن بُعد لهذه الجلسة. ويُرجى العلم بأن هذه الجلسة يجري تسجيلها وتحكمها معايير السلوك المتوقعة الصادرة عن ICANN وكذلك سياسة ICANN لمناهضة التحرش. ستُقرأ الأسئلة أو التعليقات المقدَّمة خلال هذه الجلسة في مربع الدردشة جهرًا إذا كُتبت بالشكل الصحيح كما هو مذكور. ستشمل الترجمة الفورية لهذه الجلسة كلاً من اللغة الإنجليزية والإسبانية والفرنسية. إذا كنت ترغب في التحدث خلال هذه الجلسة، يُرجى رفع يدك عبر خاصية رفع اليد في تطبيق Zoom. عندما يُسمح لك بالحديث، سوف يتم إعطاء المشاركين الافتراضيين الإذن بإلغاء كتم الصوت في برنامج زووم Zoom. سيستخدم المشاركون في الموقع ميكروفونًا ماديًا هنا للتحدث. يُرجى التكرم بذكر الاسم للتدوين في السجل وتحديد اللغة إذا كنتم ستتحدثون بلغة أخرى غير الإنجليزية. ونرجو التحدث بوتيرة مناسبة لضمان دقة الترجمة الفورية. شكرًا. والآن سأترك الكلمة لـ نيك وينبان-سميث.

نيك وينبان-سميث

شكرًا. شكرًا لك، كلوديا. أولًا، أريد أن أعرف بنفسي. بالنسبة لمن لا يعرفونني، أنا نيك وينبان-سميث من NOMINET، وهو UK ccTLD.، وأنا، في الوقت الحالي، رئيس اللجنة الدائمة المعنية بانتهاك نظام اسم النطاق في ccNSO. أعتقد أن جلسة اليوم ستكون مثيرة للاهتمام للغاية، وقد تم إعدادها مع القليل من التحضير من خلال الاجتماعات السابقة وبعض التركيز على ما أردنا أن نتعمق فيه، وما هي الأولويات الخاصة بنطاقات المستوى الأعلى لرموز البلدان ccTLD من جميع أنحاء العالم. لذا يسعدني جدًا أن أتمكن من رئاسة هذه اللجنة التي تضم خبراء متخصصين ويوجد محتوى مثير للاهتمام حقًا. ومن المفترض

أيضًا أن يكون تفاعليًا، لذا فإن الأسئلة موضع ترحيب كبير. سأحاول مراقبة غرفة Zoom، ولكنني متأكد من أن الموظفين سيبقونني على الطريق الصحيح.

نحن على جدول زمني ضيق للغاية، لذلك سأقدم زملائي في اللجنة بشكل موجز للغاية، بدءًا بالترتيب الذي يظهر على الشاشة. غابي، إن كان يمكنك أن تقدم نفسك والقليل فقط.

غابرييل أندروز شكرًا. مرحبًا، اسمي غابرييل. أنا الرئيس المشارك لمجموعة عمل السلامة العامة هنا في ICANN، وعملي اليومي هو العمل لدى مكتب التحقيقات الفيدرالي في الولايات المتحدة.

نيك وينبان-سميث شكرا يا غابرييل. كيث؟

كيث درازيك مساء الخير للجميع. اسمي كيث درازيك. أعمل لدى Verisign، وأنا مسؤول داخل الشركة عن برنامج التخفيف من انتهاك نظام اسم النطاق DNS، بالإضافة إلى إدارة فريق سياسة أصحاب المصلحة المتعددين في ICANN. وأنا سعيد جدًا لتواجدي هنا، وسعيد بالعودة إلى غرفة ccNSO. ربما يتذكرني البعض منكم عندما كنت أعمل في شركة مختلفة وحياة مختلفة أعمل فيها لدعم US.. لقد كنت واحدًا منكم. ويسعدني أن أعود. شكرًا.

نيك وينبان-سميث شكرًا لك يا كيث. مون، هل يمكنك أن تسمعنا، وهل يمكنك إيقاف كتم صوتك وتقديم نفسك، من فضلك؟

مون بيريز نعم، أستطيع أن أسمعك. اسمي هو مون. أنا مدير فني في SGNIC، لذا فأنا مسؤول بشكل أساسي عن إدارة العمليات الخاصة بسجل اسم النطاق SG.. بالإضافة إلى ذلك، تم تكليفي

في ذلك الوقت بتطوير نظام لإدارة الانتهاك، لذا فأنا أتعامل أيضًا بشكل أساسي مع جزء انتهاك النطاق. شكرًا.

نيك وينبان-سميث هذا رائع. شكرًا جزيلًا. والآن إليك يا بروس، مقدمة سريعة.

بروس تونكين اسمي بروس تونكين من رمز البلد AU..

نيك وينبان-سميث شكرًا جزيلًا، وشكرًا لك يا مون، وخاصةً على البقاء مستيقظًا. إنها ساعة غير اجتماعية إلى حد ما في سنغافورة، لذلك نقدر حقًا انضمامك إلينا عبر الإنترنت. كما ترون من الشريحة، فإن معظم الصور التوضيحية للمشاركين هي قبل جائحة كوفيد، باستثناء مون. لذلك نحن نقدر ذلك حقًا.

حسنًا، من خلال مقدمة سريعة ونظرة عامة، تبدأ هذه الجلسة بشكل أساسي باستكشاف موضوع عمليات الاحتيال عبر الإنترنت والاحتيال المالي، وخاصة التقاطع مع انتهاك أسماء النطاقات لارتكاب هذا النوع من الجرائم والانتهاكات التقنية والتأثير المجتمعي. لذا، فإن هذا الأمر يتعلق بالنظر إلى حجم المشكلة ومن ثم بعض العروض التقديمية حول الأساليب والتحديات التي لا تزال قائمة. هلا انتقلنا إلى الشريحة التالية.

لذا، هذه مجرد نظرة عامة سريعة على DASC، اللجنة الدائمة المعنية بانتهاك نظام اسم النطاق، وتذكير بأننا لسنا هنا لوضع سياسة لنطاقات ccTLD. يتم ذلك على المستوى الوطني، ولكننا هنا لتسليط الضوء على القضايا المهمة وتعزيز الفهم والوعي. ونريد أن يكون لدينا حوار مفتوح وبناء. ولكن بطبيعة الحال، في نهاية المطاف، نحن مهتمون بشكل أساسي بخفض مقدار انتهاك سجلات ccTLD الخاصة بنا ومساعدة الجميع على تحقيق هذا الهدف. الشريحة التالية من فضلك.

لذا، كنوع من إعداد المشهد، في عامي 2002 و2024، أجرينا مسحًا عالميًا لنطاقات المستوى الأعلى لرموز البلدان ccTLD. وهذه كلمة قانونية مثيرة للاهتمام هنا، وهي

التفرع. من حيث سياسات ICANN، فإن نطاقات gTLD تقع بشكل ثابت ضمن نطاق سياسة ICANN والتعريف الفني لانتهاك نظام اسم النطاق DNS. ولكن ما ظهر من خلال هذه الاستطلاعات هو أن العديد من نطاقات ccTLD لا تحتوي على هذا، كما يعتبره البعض، نوعًا من التمييز الدلالي أو الاصطناعي بين أنواع معينة من الانتهاكات وأنواع أخرى معينة من الانتهاكات. معظمنا يعتبر الانتهاك انتهاك. وقد اتضح أن المحتوى الإجرامي، على سبيل المثال الاحتيال، يشكل قضية كبرى. وفي الواقع، فإن هذا الأمر قابل للتنفيذ ويعتبر أمرًا يجب على السجل التدخل فيه في مواقف معينة. أردت أن أسلط الضوء مرة أخرى على اجتماعنا في كيغالي، حيث سمعنا بشكل خاص من الأفريقيين ومسؤولي التسجيل النيجيريين على وجه الخصوص عن وباء عمليات الاحتيال المتعلقة بالعملات المشفرة. إنها مجرد عملية احتيال مطلقة تستهدف المستهلكين والمواطنين الضعفاء في هذا البلد. في المملكة المتحدة، حيث أعيش، يشكل الاحتيال 40% من إجمالي الجرائم، وهي نسبة ضخمة. إنه أكبر أشكال الجريمة. نسبة 80% من عمليات الاحتيال في الدفع تنشأ إما من وسائل التواصل الاجتماعي أو من مواقع الويب المزيفة. لذا فإن هذا المجال يقع مباشرة ضمن نطاق اختصاص العديد من سجلات ccTLD. وهناك درجة عالية من التداخل فيما يتعلق بالتعريف الفني لانتهاك نظام اسم النطاق DNS، الذي يتضمن التصيد الاحتيالي. إنه العنصر الرئيسي لانتهاك DNS في العالم. ومن الواضح أن استخدام رسائل البريد الإلكتروني الاحتيالية يعد نقطة دخول لمرتكبي الجرائم المالية. في اجتماعنا الأخير في سياتل، استقرينا على هذا الموضوع. لذا كنت سأنتقل الآن إلى مناقشات اللجنة. وبعد أن قلت ذلك، سأتابع مع الشريحة التالية، وهي الشريحة الخاصة بالتعريف. الرسائل الخادعة عبارة عن دعوة أو طلب أو إخطار أو عرض احتيالي يهدف إلى الحصول على معلومات شخصية أو أموال أو اختبار منفعة مالية عن طريق الخداع. في كثير من الأحيان، ولكن ليس دائمًا، يكون النطاق المسجل بشكل ضار جزءًا من ذلك. الشريحة التالية فقط. لذا فإن هذه الجلسة هنا هي بمثابة جلسة تمهيدية. ونخطط للقيام بمزيد من العمل في اجتماعات ICANN اللاحقة. ويمكنك أن ترى أننا سنوسع هذا الأمر إلى محادثة أوسع بين أصحاب المصلحة من مختلف المجتمعات. هناك Mentimeter سريع هنا في بداية الجلسة. لذا إذا كان بوسعنا المضي قدمًا. سأعطي الجميع فرصة صغيرة. هناك استطلاعان على Mentimeter. لذا أحاول أن أعطي الجميع فرصة لالتقاطها. أحد الأشياء التي أعتقد أننا نقوم بها بشكل جيد للغاية في ccNSO هو استخدام استطلاعات الرأي التفاعلية هذه. يساعد

الناس. وهو ما يشكل أغلبية ccNSO ويسمح للناس بالقيام بذلك بشكل جيد. لذا دعونا ننتقل إلى السؤال إذا كان الجميع مستعدين. الشريحة التالية. حسنًا، السؤال هو سؤال سهل. إلى أي مدى يعتبر سجلك جاهزًا بشكل جيد للكشف عن انتهاك اسم النطاق المرتبط بالجرائم المالية؟ أعط الناس فرصة لـ... حسنًا، هذه ليست دراسة علمية دقيقة. إنه مجرد نوعًا ما درجة حرارة الغرفة، ونكهة حجم المشكلة والفهم. وبناء على ذلك، أود أن أترك الكلمة لغابي ليقدم عرضه. غابي، الكلمة لك.

غابرييل أندروز

حسنًا. هل يمكنني رؤية الشريحة التالية؟ ممتاز. شكرًا. في سياتل، كنت أتحدث مع نيك وذكرت له أن تقرير مكتب التحقيقات الفيدرالي السنوي حول الجرائم على الإنترنت لم يكن من المقرر نشره قبل سياتل وأنه سيتم نشره بعد ذلك بفترة وجيزة. وذكر لي أنه قد يكون من المثير للاهتمام التحدث عن هذا الأمر معكم جميعًا. لذلك أردت اغتنام الفرصة وأشكركم على الفرصة. تأتي هذه البيانات من بوابة مركز شكاوى الجرائم على الإنترنت. وما يعنيه هذا هو أنه في كل مرة يأتي إلينا ضحية ويريد أن يخبرنا بأنه تعرض لانتهاك، فإننا نقوم بتوجيهه عبر بوابة واحدة تساعدنا حقًا في تبرير الموارد التحقيقية التي نضعها لربط هذه الحالات معًا والضحايا معًا. ولكنه يوفر فائدة إضافية تتمثل في تزويدنا ببعض الإحصائيات الجيدة التي يمكننا بعد ذلك نشرها على أساس سنوي. الشريحة التالية.

أريد أن أعترف بأنني مجرد شرطي من بلد واحد، ولكن على الرغم من ذلك، عندما نجري هذه الحسابات، نرى أننا نتلقى بالفعل شكاوى من أكثر من 200 دولة حول العالم، على الأقل في عام 2024. حسنًا، كما تعلم، نيك، كانت المملكة المتحدة مسؤولة عن أكثر من 100,000 حالة، على سبيل المثال فقط. وهذا يعكس حقيقة أن الجريمة الإلكترونية عالمية، أليس كذلك؟ لذا أعتقد أنه على الرغم من أنني أتحدث عن إحصائيات من الولايات المتحدة، فإن هذا يمثل إلى حد كبير ما يراه نظرائي في جميع أنحاء العالم أيضًا. الشريحة التالية.

لذا ما نقوم به هو حساب عدد الشكاوى التي نتلقاها، ثم نحاول أيضًا تلخيص مقدار الخسارة المرتبطة بكل فئة من الشكاوى والجرائم التي نسمع عنها. وقد سلطت الضوء على عدد قليل هنا. آمل أن تتمكنوا من قراءته جيدًا. ولكن على اليسار، عندما تنظر إلى عدد الشكاوى، يمكنك أن ترى أن التصيد الاحتيالي مسؤول عن عدد أكبر بكثير من الشكاوى مقارنةً بأي شيء آخر نسمع عنه. وهذا منطقي. نعلم أن التصيد الاحتيالي يحدث طوال الوقت. وكما

قلت يا نيك في وقت سابق، فإن هذا هو في الواقع ناقل التطفل الأولي أو الطريقة الأولية التي يتم بها ارتكاب الكثير من الجرائم الأخرى. وبعد ذلك عندما تنظر إلى اليمين وتحاول أن تحسب الإجمالي، حسنًا، أين يحدث الخسارة؟ الفئة الأعلى هنا هي الاحتيال الاستثماري، والذي يشار إليه أيضًا باسم الاحتيال الاستثماري في العملات المشفرة. وهكذا انتبهت عندما تحدثت عن سماعي من نيجيريا عن هذا الأمر وعن كونه وباءً. إنه وباء. وهذا مسؤول عن خسارة تزيد عن 6.5 مليار دولار في الولايات المتحدة في العام الماضي وحده، أي في عام 2024. وهو مسؤول أيضًا عن انتحار الضحايا عندما يخسرون مدخرات حياتهم. سنتعمق في هذا الأمر قليلًا. ولكنني أردت أيضًا أن أقضي بعض الوقت في الحديث عن اختراق البريد الإلكتروني الخاص بالأعمال، وهو مجرد فئة فرعية من التصيد الاحتيالي، ثم أتحدث قليلًا عن برامج الفدية. لأنه على الرغم من أن الخسارة هناك تصل إلى 12 مليونًا فقط، إلا أنها في الواقع أسوأ من ذلك بكثير. أعرف أن هذا ليس احتياليًا، لكنه كان يستحق لحظة. حسنًا، فلننتقل إلى الشريحة التالية. وسنتحدث عن اختراق البريد الإلكتروني الخاص بالعمل.

هذا هو التصيد النمطي حيث ينتحل شخص سيء شخصية شخص يشبه الرئيس التنفيذي، ولديه القدرة على بدء التحويل البنكي. وهذه رسالة بريد إلكتروني حقيقية من BEC عندما كنت أعمل على هذا الانتهاك في عام 2015 أو نحو ذلك. لقد حصلنا على إذن من الضحية لاستخدام هذا لأغراض تعليمية. إذا لاحظت ذلك، لا أتذكر ما إذا كانت هذه شريحة أخرى أم لا، ربما يمكنك اللعب معي وسنعود مرة أخرى إذا لم تكن كذلك. ولكن انقر مرة واحدة فقط لمعرفة ما إذا كان هناك تسليط ضوء. حسنًا، أنا مستعد. حسنًا، ها نحن ذا. لذا يمكنك أن ترى أن الموضوع الفعلي هنا كان انتحال شخصية شركة Fly Jet Edge. لقد قاموا بتسجيل اسم نطاق مشابه للاسم المتجانس. وباعتباري محققًا، فإن أحد الأشياء الأولى التي أردت القيام بها هي أن أقول، حسنًا، ما هو المتاح للعامة حول اسم النطاق هذا؟ لذلك عليك إجراء بحث WHOIS. وفي ذلك الوقت، ربما كنت قد رأيت السجل بهذا الشكل. وأحد الأسباب التي تجعلني أنظر إلى هذا هو أنني أريد أن أعرف أين يمكنني إرسال إجرائي القانوني؟ هل هم في بلدي؟ هل هم في بلد آخر؟ أين سنذهب للتحقيق في هذا الأمر؟ تفضل، التالي. في انتظار التالي. ها نحن ذا. رائع.

إن عملية تقديم الإجراءات القانونية تستغرق وقتًا طويلًا. لذا دعنا نقول بعد أسبوعين أو ثلاثة أسابيع، سأحصل على الاستدعاء. لقد أرسلته. سأحصل على النتائج. أحد الأشياء التي

قد أسأل عنها هو ما هي أسماء النطاقات الأخرى التي سجلها هذا الرجل السيئ؟ بالإضافة إلى هذا الذي يستهدف هذه الضحية التي تواصلت معي. وقد أرى أنه قد يكون هناك عشرات أو عشرات من أسماء النطاقات الأخرى التي سجلوها، والتي باستخدام عقلي المحقق فائق الذكاء، يمكنني أن أستنتج أنها مجرد خطأ إملائي بسيط لشيء ربما يكون حقيقيًا. والآن وظيفتي هي في خضم محاولة القيام بهذا التحقيق، أريد أيضًا أن أعلم هؤلاء الضحايا المحتملين أنهم مستهدفون بشكل نشط من قبل الرجل السيئ، أليس كذلك؟ وأحد الأشياء التي قد أفعلها هو أنني قد لا أخصص الوقت لإجراء عملية قانونية إضافية لمدة أسبوعين أو ثلاثة أسابيع لكل أمين سجل مرتبط بتلك النطاقات الضحية الإضافية. ولكن إذا تمكنت من العثور على بعض أرقام الهواتف الجيدة من WHOIS حول هؤلاء الضحايا المحتملين، فقد أكون قادرًا حقًا على منع المزيد من الضرر. حسنًا، انقر.

على نحو مماثل للغاية مع برامج الفدية، كنت أتحدث مع وكالتي الشقيقة، CISA، وهي المسؤولة عن حماية البنية التحتية الحيوية في الولايات المتحدة. دعونا ننتقل إلى الشريحة التالية هنا أيضًا. وأردت فقط أن أسلط الضوء على أن هذه فئة مختلفة تمامًا من الجرائم. لا يتعلق الأمر بالاحتيال، ولكن ما يتعين عليهم فعله في مهمتهم مشابه جدًا لما وصفته للتو. إنهم أيضًا في وضع يسمح لهم بمحاولة منع الضرر. وفي حالتهم، قد يكون لديك باحثو الأمن السيبراني الذين يراقبون خوادم برامج الفدية المعروفة. وبناءً على ملاحظاتهم التاريخية، فإنهم يعرفون أنه عندما يتم رؤية ضحية جديدة لأول مرة وهي تقوم بإرسال رسائل إلى البنية التحتية الخاصة ببرامج الفدية، فبعد 24 أو 48 أو 72 ساعة التالية، قد يتم نشر برامج الفدية على شبكة الضحية. وبعد ذلك بفترة وجيزة، سيتم تفعيله وسيكون لديهم يوم سيء. لذلك سوف يخبرنا الباحثون بذلك. وسوف يتواصلون مع وكالة الأمن السيبراني والبنية التحتية، ومكتب التحقيقات الفيدرالي، وقد عملنا معًا على ذلك لفترة من الوقت. وسيقولون، مهلا، تم رصد عنوان IP الجديد الخاص بهذه الضحية وهو يتواصل مع هذا الرجل السيئ المعروف. ثم لدى CISA الوقت الكافي لتحديد مدى السرعة التي يمكنهم بها تحويل معرف الإنترنت هذا إلى محادثة. ولهذا السبب فقد اعتمدوا أيضًا بشكل كبير على توافر السجلات، والسجلات العامة، لتحويل معرفات الإنترنت تلك بسرعة إلى معلومات اتصال في العالم الحقيقي. وهذا أمرٌ بالغ الأهمية. أعتقد أنهم وفروا أكثر من ثمانية مليارات ونصف المليار دولار من مدفوعات الفدية المحتملة في العام الماضي وحده، وذلك عبر أكثر من 2400 إشعار للضحايا. حسنا، التالي.

أحاول التحرك بسرعة هنا، مع العلم أننا نسير على مدار الساعة. احتيال الاستثمار في العملات المشفرة. حسنًا، لقد أشرنا إلى هذا من قبل. يبدو أنك سمعت عنها بالفعل من نيجيريا. وفي الولايات المتحدة، مرة أخرى، تعد هذه الفئة من الخسائر الأكثر ضررًا التي نشهدها، إذ تتجاوز ستة مليارات ونصف المليار دولار. وكان أعلى رقم تالٍ هو [غير مسموع] عند أقل من النصف. دعونا ننقر. أعتقد أن الجميع في هذه الغرفة من المحتمل جدًا أن يكونوا مستهدفين من قبل أحد هؤلاء في البداية. يبدأ الأمر دائمًا برسالة WhatsApp أو Signal أو أي منصة دردشة تختارها. ومن غير المؤذي دائمًا أن تبدأ محادثة مع شخص يحاول الدخول في محادثة. وهناك بعض التظاهر. ربما يتظاهرون بأنهم طبيبك البيطري أو طبيبك أو شخص آخر وأنه كان صديقًا. وهذا مجرد خطأ صادق أنهم يرسلون لك الرسائل النصية بدلًا من شخص آخر. وسوف يقضون الكثير من الوقت في محاولة تحويل ذلك إلى محادثة، وتحويل تلك المحادثة إلى ثقة. وفي وقت لاحق، أدرج في المحادثة حقيقة أنهم حققوا للتو قدرًا كبيرًا من المال على منصة استثمار العملات المشفرة هذه أو تلك. إذا اشتريت هذا، فقد تستثمر فيه بنفسك بعد ذلك بوقت قصير جدًا. إذا قمت بالاشتراك في المزيد من المحادثات، فقد تعتقد أنك تكسب الكثير من المال وتضع المزيد والمزيد من مدخرات حياتك في هذا، كما حدث. انتقل وانقر على التالي.

وعندما يفعلون ذلك، فإنهم سيديرون منصات تبادل العملات المشفرة المزيفة بأنفسهم. يمكن تحديثها بالبيانات الحية في الوقت الحقيقي. لذا يبدو الأمر حقيقيًا وأصيلًا للغاية بالنسبة للضحايا. عندما أتحدث إلى وكلاء القضية الذين يحققون في هذا الأمر، وسوف ننتقل إلى الشريحة التالية هنا، يخبروننني أن الأشرار، مستعدون للهجوم التالي. يخبروننني أن الأشرار سوف يقومون بتسجيل مئات النطاقات بشكل خبيث في وقت واحد من أجل الترويج لتلك البورصات المزيفة للعملات المشفرة. لذا أردت فقط تسليط الضوء على هذه الحقيقة، وهي أنه إذا كنت تلاحظ أن هناك تسجيلات جماعية يتم إجراؤها من خلال نطاق ccTLD الخاص بك، فحتى لو لم تكن هذه النطاقات نفسها نطاقات ccTLD، فإنها يمكنها استخدام نطاقات ccTLD كجزء من هذا وسوف تفعل ذلك. إن الحجم الهائل لهذه البيانات يسمح لهم بتعزيز هذه التبادلات. حتى مع إزالة أحد النطاقات، يتم تحويلها إلى النطاق التالي ثم التالي إلى التالي.

والجزء الصعب بشكل خاص في هذا الأمر هو أنه عندما ينظر المحققون إلى هذا الأمر، في كثير من الأحيان لا يكون المسجلون الذين يتم استخدامهم موجودين محليًا بالنسبة

لوكالات إنفاذ القانون وهناك بعض التحديات التي تنشأ بسبب ذلك وسنمضي قدمًا. وانقر للانتقال إلى الشريحة التالية الآن. عندما نستخدم معلومات متاحة للعامة مثل تلك الموجودة على يسار هذا الرسم التخطيطي الصغير الذي قمت بإنشائه مثل موارد Google أو WHOIS، يمكننا إجراء هذه الفحوصات في دقائق، أليس كذلك؟ ثواني أو دقائق. نحن كرجال شرطة لدينا السلطات اللازمة لإرسال استدعاءات قانونية إلزامية أو أوامر من المحكمة، ولكن هذا يحرك الجدول الزمني إلى أيام أو أسابيع، وربما حتى شهر للحصول على مذكرة تفتيش. وعندما يتعلق الأمر بعبور الحدود الدولية، فإننا نعتمد الآن على الأداة الوحيدة المتاحة لنا، وهي طلبات معاهدة المساعدة القانونية المتبادلة. ومن خلال تجربتي، استغرق الأمر مني ما بين ستة إلى اثني عشر شهرًا في المتوسط عندما قمت بذلك في الماضي. إنه ليس مناسبًا جدًا للتحقيقات السريعة. وبالتالي، فإن النقطة الرئيسية التي أود التأكيد عليها هي أنه عندما نتمكن من قبول أشياء مثل بيانات WHOIS طواعية من مشغلي ccTLD، حتى لو لم نكن في نفس البلد، فإن هذا يمكن أن يجعل وظائفنا أسرع بكثير في محاولة معرفة المزيد عن الأشرار. لذا دعونا ننتقل إلى ما أعتقد أنه الشريحة الأخيرة لدي. ها نحن ذا.

حسنًا، إليكم ملخصًا سريعًا للنقاط التي كنت أتناولها هنا. تُعد بيانات WHOIS مفيدة للغاية لرجال الشرطة في جميع أنحاء العالم عندما نحاول معرفة المكان الذي يجب أن نوجه إليه عملية الإجراءات القانونية أو أوامر المحكمة وما إلى ذلك. إذا كنت تستخدم البائعين بنفسك، فيرجى إدراجهم. أنا حقًا لا أريد أن نرسل العملية القانونية إلى الكيان الخطأ لمجرد أننا اعتقدنا أنه أمين سجل، ولكن في الحقيقة إنه شيء تحت أمين السجل. ترغب وكالات السلامة العامة بشدة في أن تتمكن من استخدام WHOIS لمنع إلحاق الضرر بالضحايا. إن الاحتيال في الاستثمار في العملات المشفرة هو في الواقع أمر سيء للغاية ورهيب، ويتضمن التسجيل بكميات كبيرة للترويج للتبادلات المزيفة. وأخيرًا، هناك الاستجابات الطوعية للسلطات المحلية الأجنبية – إنفاذ القانون الأجنبي. إذا كانت المعلومات من بلد تحترمه وتعتقد أنك تستطيع الوثوق به، فإن الإفصاح الطوعي يمكن أن يساعدنا حقًا، على الرغم من أنني أعلم أنه دائمًا خيار وتقدير المستخدم. حسنًا. لذا، أشكركم جميعًا على اهتمامكم. آمل أن يكون هذا مثيرا للاهتمام وأنا ممتن للغاية حتى للفرصة التي أتيحت لي للتحدث. نيك، عودة إليك.

نيك وينبان-سميث شكرا جزيلا لك، غابي. هل هناك أي أسئلة فورية؟ أعتقد أن الشيء الوحيد الذي كنت سأقوله هو أن الكثير من الأمثلة تبدو وكأنها نطاقات gTLD، لكنها تؤثر على نطاقات ccTLD. ومن وجهة نظري، ورغم أنني قد لا أعترف، مع كل الاحترام، بسلطة الولايات المتحدة، فإنني إذا تلقيت شيئًا من مكتب التحقيقات الفيدرالي وكان يشير في الأساس إلى وجود عملية احتيال، فلن أضعه في سلة المهملات. هناك سياسات أخرى داخلية لكل نطاق ccTLD. إذا كان لديك سبب وجيه لإجراء مزيد من التحقيق، فهناك عمليات لمعظم نطاقات ccTLD التي لن تتطلب عمليات MLAT، لأنه إذا تمكنا من رؤية، على سبيل المثال، أن البيانات المسجلة مزيفة بشكل واضح، فهناك عمليات أسرع بكثير من تلك التي تتبعها معظم السجلات المسؤولة طواعية. وآمل أن نتمكن من التحدث أكثر عن هذا الأمر. ولكن دعونا ننتقل إلى كيث على يساري.

كيث درازيك شكرًا جزيلاً لك، نيك. مرحبًا بكم جميعًا. كيث درازيك مع Verisign. أنا هنا اليوم لأقدم مقدمة لمبادرة جديدة تسمى منتدى البنية التحتية للإنترنت. وسوف أصل إلى التفاصيل في لحظة. أود أن أقدم القليل من السياق والخلفية حول سبب كون هذا شيئًا ندعمه جنبًا إلى جنب مع عدد قليل من الآخرين. في عام 2022، أدركت سجلات gTLD ومسجلوها أننا بحاجة إلى اتخاذ خطوة إلى الأمام واتخاذ المبادرة للتعامل مع موضوع انتهاك DNS كما تمت مناقشته في مساحة ICANN. أعتقد أنكم جميعًا تعلمون أن سجلات gTLD وأمناء السجلات لديهم عقود مع ICANN. لقد كان هناك نقاش لمدة 10 سنوات حول موضوع انتهاك نظام اسم النطاق DNS. وأدركنا أن هناك حاجة إلى القيام بشيء ما.

لذا، فقد انخرطنا طواعية مع ICANN، وعرضنا وطلبنا تحمل التزامات تعاقدية جديدة قابلة للتنفيذ للتعامل مع انتهاك نظام اسم النطاق DNS. ومن خلال هذه العملية، قمنا بتعريف انتهاك نظام اسم النطاق DNS مع ICANN في عقودنا على أنها انتهاك تقنية للتصيد الاحتيالي، والزراعة، والبرامج الضارة، وتوزيع الأوامر والتحكم في شبكات الروبوتات، والبريد العشوائي عندما يتم استخدام البريد العشوائي كآلية توصيل لتلك الأربعة الأخرى. وبعد أن قمنا بتحديد المصطلح، مصطلح انتهاك نظام أسماء النطاقات المحدد في عقودنا،

أدركنا أيضًا أنه سيكون هناك ضغط مستمر على ICANN للتدخل في الأضرار المتعلقة بالمحتوى. بالنسبة لمن قد لا يكونون على دراية تامة، فإن لوائح ICANN تحظر عليها التدخل في تعديل المحتوى أو أي شيء من هذا القبيل. ولذلك أدركنا أن هناك حاجة إلى تطوير نقطة أخرى لإشراك أصحاب المصلحة المتعددين، ومسار موازٍ لمناقشة الأضرار عبر الإنترنت لتشمل المحتوى، ولكن يجب أن يكون ذلك موجودًا خارج نطاق ICANN، خارج مظلة ICANN. وبالتوازي مع المناقشات حول مفاوضات العقد، اجتمعت العديد من سجلات gTLD وبدأوا في الحديث عن الحاجة إلى تطوير ما يُعرف الآن بمنتدى البنية التحتية للإنترنت. لقد كانت Verisign وPIR وIdentity Digital وGoogle وAmazon وCloudFlare هي الشركات الست التي اجتمعت معًا مدركة أن هذا أمر يستحق المتابعة، وأننا أردنا إشراك مشغلي البنية التحتية للإنترنت المشاركين في المحتوى والمضيفين وشبكات توصيل المحتوى وما إلى ذلك، لجلبهم إلى طاولة المفاوضات والبدء في الحديث عن كيفية عملنا كمشغلي البنية التحتية للإنترنت بشكل أفضل معًا للتعامل مع الأضرار عبر الإنترنت وتخفيفها على نطاق أوسع من المصطلح المحدد داخل مساحة ICANN.

وهذه هي المبادرة التي بدأت بجدية تامة في العام الماضي. لقد عقدنا اجتماعنا الأول وجهًا لوجه في الأسبوع الأول من شهر فبراير/شباط في أمستردام هذا العام. كان لدينا 53 مشاركًا يمثلون 38 منظمة – أبطأ، آسف – 38 منظمة خلال اجتماع استمر يومين، والذي أعتقد أنه لاقى استحسانًا كبيرًا. نحن، الشركات الست التي اجتمعت معًا لبدء هذا، عملنا بشكل وثيق للغاية مع شبكة سياسة الإنترنت والاختصاص القضائي، وأود أن أتقدم بالشكر إلى برتراند دو لا شابيل، الذي معنا هنا اليوم. وهو بمثابة المنسق والميسر الرئيسي لهذا الجهد الذي يبذله منتدى البنية التحتية للإنترنت، ويعمل أيضًا مع ICO ومبادرتهم الرئيسية لنظام أسماء النطاقات DNS وتحالف البنية التحتية للإنترنت، I2C، ومقره في أمريكا الشمالية. وهذا هو الأساس الذي تقوم عليه المجموعة الأساسية من الميسرين، أولئك الذين يعملون على تحقيق أهداف IIF.

لذا، بعد الخروج من اجتماع أمستردام، كان من المهم حقًا بالنسبة لنا أن نؤكد على أن هذا المسعى يستحق العناء، وأن هناك إجماعًا، خاصة بين مضيفين الويب وشبكات توصيل المحتوى ومقدمي خدمات السحابة الذين لا يشاركون عادةً في مساحة ICANN ما لم يكن

لديهم سجل أو أمين سجل، ولكن حقًا لإشراك طبقة المحتوى في هذه المحادثات. لقد كنا بحاجة ماسة إلى التأكد من وجود اهتمام ونوع من الاستعداد للالتزام بالمشاركة في معرفة كيفية العمل معًا بشكل أفضل بطريقة تعاونية، ومشاركة المعلومات، وتحديد الموضوعات الملموسة التي تمكننا من المساعدة في التخفيف من الأضرار عبر الإنترنت ضمن أدوارنا ومسؤولياتنا وقدراتنا التقنية، اعتمادًا على الضرر الفعلي الذي نحاول معالجته. وبناءً على اجتماع أمستردام، حددنا أربعة مسارات عمل، يركز أحدها على السياسة القانونية والتطورات التنظيمية لتشمل، في ذلك الوقت، تنفيذ اتفاقية الخدمات الرقمية ومتطلبات الشفافية، ونقل نظام المعلومات الأمنية 2 ومعرفة قضايا عملائك، والقانون العام لحماية البيانات GDPR ومشاركة المعلومات. كان هذا مسارًا تم تحديده للمساعدة حقًا في إعلام ودعم بعض الأعمال الأخرى التي تم استهدافها بشكل أكبر في المسار الثاني وهي القضايا التشغيلية والأتمتة، وكيف نطور أنظمة يمكنها تسهيل تبادل المعلومات، وتوجيه تقارير الانتهاك مع حلقات التغذية الراجعة، بحيث يكون لدى الجهات الفاعلة المختلفة في المكدس القدرة على التواصل بشكل أكثر فعالية وكفاءة، لمساعدتنا جميعًا في معالجة الأضرار بشكل أكثر فعالية. ثم هناك مساران جوهريان، الأول يركز قليلًا على مواد الاعتداء الجنسي على الأطفال CSAM والصور الحميمية غير المقبولة NCII، ولكن في الواقع يركز هذا الفريق على الحديث عن دور المبلغين الموثوق بهم والمبلغين الموثوق بهم في نظام التخفيف من الانتهاك. والمسار الأخير من الأربعة هو التصيد الإضافي، والذي يشير بشكل أساسي إلى أن التصيد، كما ذكر غابي، هو أحد أكبر أنواع ناقلات الاحتيال، لكنه يتيح العديد من أنواع الاحتيال الأخرى والانتهاك والأضرار عبر الإنترنت. وهذه كانت الفئة الأخرى. لذا فهي مبادرة مثيرة حقًا. نحن في هذه المرحلة حيث نبدأ في الرغبة في توسيع العضوية، ولكن أيضًا المشاركة، يجب أن أقول، إنها ليست منظمة عضوية، لتوسيع المشاركة، ولكننا ندرك أيضًا أننا بحاجة إلى الحفاظ على التوازن بين مشغلي DNS التقليديين والتأكد من حصولنا على طبقة المحتوى والمضيفين المعنيين.

وسأختتم هنا بالقول إن هذه في نهاية المطاف مبادرة يقودها القطاع حاليًا. إنها صناعة حقيقية في هذه المرحلة. نتعاون مع مقدمي الخدمات الذين يساهمون في تسهيل التخفيف من الأضرار عبر الإنترنت. لذا، لدينا جوهر جيد في هذه المرحلة. لكن الخطة هي توسيع هذا العمل لضمان مشاركة أصحاب المصلحة المتعددين، وللتأكد من أننا نتعامل مع مجموعات المصالح الأخرى والمجموعات الأخرى ذات الخبرة. وهذه هي الخطوة التالية

بينما نمضي قدمًا في إنجاز بعض هذا العمل، والتقدم في هذا العمل، وهي التأكد من أننا نتمتع بمشاركة أصحاب المصلحة المتعددين حتى نتمكن من ضمان أن ما نقوم به مستنير بشكل جيد. بذلك، سأتوقف إذن عند هذا الحد. شكرًا لك يا نيك.

نيك وينبان-سميث

شكراً لك يا كيث. لذا فإن جزءًا من سبب تضمين هذا الموضوع في هذا العرض هو أنني أعتقد أننا جميعًا ندرك حقيقة مفادها أن مجرد التصرف على مستوى اسم النطاق لا يعدو أن يكون نوعًا من الأشياء التخريبية. أنت في الواقع لا تتناول المحتوى بشكل أساسي. لذا فإن الوصول إلى مستضيف موقع الويب الذي تتم فيه عمليات الاحتيال أو التصيد الاحتيالي أو أي ضرر آخر عبر الإنترنت هو في الواقع الهدف النهائي، لأن النشاط التخريبي الذي يمكنك القيام به كمشغل ccTLD لا يمنع أسماء النطاقات الأخرى، سواء كانت gTLD أو ccTLD، من الظهور بسرعة كبيرة ثم الإشارة إلى نفس الشيء. لذا أعتقد أن هذا النوع من المنظور مثير للاهتمام للغاية ويجب أن نضعه في الاعتبار بينما نتجه نحو المزيد من المناقشات حول هذه القضايا المتعلقة بالمحتوى في نهاية المطاف. إذن هذا هو الأمر. والآن دعونا ننتقل إلى مون في سنغافورة لإجراء دراسة حالة صغيرة حول كيفية إنشائهم لمبادرة لمحاربة الجرائم المالية. شكرا لك، مون. الكلمة لك.

مون بيريز

شكرًا لك يا نيك. الشريحة التالية من فضلك. حسنًا، لوضع الأمر في سياقه، نحن جميعًا نعلم أن الجريمة المالية تشكل قضية كبرى. وهذا يؤدي إلى خسائر مالية ويضر بالثقة العامة في اسم النطاق SG.. لقد تمكنت من الحصول على التقرير من أحد محركات البحث المحلية في سنغافورة. وكان هناك 8000 محاولة تصيد في عام 2022. لحسن الحظ، لم يكن أي منهم من SG.. كانت معظمها من نطاقات ccTLD أخرى. 80% من محاولات التصيد كانت تستهدف البنوك والخدمات المالية والحكومة والخدمات اللوجستية. الشريحة التالية من فضلك. وهذه هي الانتهاكات التي تثير قلق SGNIC. ولكي نضع الأمر في سياقه، فإن المجموعة الأولى تتضمن الانتهاكات التي تدركها ICANN أو التي تشعر بالقلق بشأنها بشكل أكبر. التصيد الاحتيالي والبريد العشوائي وشبكات الروبوتات وهجمة تزوير المواقع الإلكترونية. المجموعة الثانية هي الانتهاكات التي تثير قلق SGNIC. لذا فإن

الأشياء التي تحمل علامات النجمة هي الأشياء التي تشعر SGNIC أنه ينبغي لنا أن نفعل المزيد بشأنها. وفي وقت لاحق، سأشارككم ما هي الأشياء الإضافية التي قمنا بها. والأمر الأخير هو أن هذه ليست انتهاكات حقيقية، ولكنها نوع من المؤشرات التي يستخدمها فريقنا للكشف عن العلامات المبكرة للانتهاكات المحتملة. الشريحة التالية من فضلك.

حسنًا. هذه هي التدابير الوقائية والكشفية التي اتخذتها SGNIC. أولًا، لدينا الهوية التي تم التحقق منها في SG. وهذا يضمن أن تسجيل اسم النطاق يخضع للتحقق باستخدام SINGPASS، وهي الهوية الرقمية الوطنية لسنغافورة. وهذا يقلل من سرقة الهوية. لذا، في الأساس، هذه هي عملية KYC الخاصة بنا. ثانيًا، لدينا قفل السجل، وهي ميزة أمان مجانية لمساعدة مسجل Azure في التخفيف من خطر اختطاف اسم النطاق أو التعديل غير المصرح به. وأخيرًا، لدينا نظام إدارة الانتهاكات. هذا نظام داخلي يراقب المواقع الإلكترونية الضارة المتعلقة بالتصيد الاحتيالي أو البرامج الضارة، وبالتالي، فإننا ننبه أصحاب المصلحة لاتخاذ الإجراءات اللازمة. الشريحة التالية من فضلك.

حسنًا، سأنتقل إلى عمق نظام إدارة الانتهاك. لذا، في الأساس، تم تطوير هذا داخليًا. وما يفعله هو اكتشاف وتتبع انتهاك اسم النطاق، والتي ذكرتها، في الغالب البرامج الضارة والتصيد الاحتيالي. ويقوم أيضًا بالتحقق من معلومات التسجيل غير الصحيحة أو المشبوهة. ويقوم أيضًا بالتحقق من استخدام مياه DNS وتسجيل الروبوت. لذا فإن النظام يقوم بشكل أساسي بالإشارة إلى أي من انتهاكات اسم النطاق المحتملة هذه. وعندما يتم تحديدها، نتمكن من التحقق من صحتها، ثم إذا كانت حالة مؤكدة، فسوف نقوم بإخطار أصحاب المصلحة، مثل المسجل وأمين السجل ومزود الاستضافة، لاتخاذ الإجراء اللازم. في البداية، تعاونت SGNIC مع محرك بحث محلي لتوفير رأي الخبراء، لأننا لم نكن على دراية بكيفية اكتشاف البرامج الضارة والتصيد الاحتيالي في ذلك الوقت. ولكن بعد ذلك، ظهرت قنوات تجارية توفر بيانات الحلول. ونتيجة لذلك، تولت SGNIC الدور. والآن، تم تضمينه في النظام. الشريحة التالية من فضلك.

وهذه هي الميزة الأخرى لنظام إدارة الانتهاك. وبشكل أساسي، فهو يكتشف التسجيل غير الصحيح أو المشبوه. ما يفعله هو أنه عند إعطاء رقم تسجيل الشركة، يقوم النظام بالتحقق منه مقابل قاعدة بيانات تسجيل الشركة، ثم يستخرج اسم الشركة. وبناءً على اسم الشركة، نقوم بعد ذلك بمقارنته مع اسم الشركة المسجلة للتأكد من أن التسجيل وهمي أم لا. الشريحة

التالية من فضلك. إذن هنا جزء آخر من AMS. لذا، في الأساس، هذه مجرد تقارير CQ. وبالتالي، فإنها تزودنا بمعلومات حول بعض الهجمات والتطبيقات الشائعة المستهدفة. بطريقة ما، هذا يمنحنا إحساسًا بأنواع الانتهاكات الشائعة، وما هي عوامل الانتهاك الشائعة، أو ما إذا كان هناك أي ارتفاع في انتهاكات أسماء النطاقات التي اكتشفناها. الشريحة التالية من فضلك. إذن ما الذي جلبته كل هذه الجهود إلى SGNIC؟ أولًا، لم نسجل أي حوادث تتعلق بسرقة اسم النطاق. وأيضًا، لأن لدينا نظامًا الآن، فنحن قادرون على قياس معدل الدقة لدينا. لذا فإن ما نقوم به هو التأكد من أننا نحافظ على حل 80% من الحالات شهريًا. وهذا هو هدفنا حتى الآن. ثالثًا، لقد أصبحنا على علم جيد بالتهديدات المستمرة أو الناشئة. ولكي نسلط الضوء على حادثة واحدة جديرة بالملاحظة، فقد تم بناء AMS لأول مرة في عام 2010. وبعد مرور عدة سنوات، وقع حدث في يوليو/تموز 2012 حيث تم استغلال منصة استضافة ويب شهيرة. وكان هذا ملحوظًا جدًا في AMS لأننا تمكنا من رؤية حوالي 100 اسم نطاق sg. تُستخدم في عمليات التصيد الاحتيالي. وبفضل AMS، تمكنا من العثور على مزود استضافة مشترك. لذا ما فعلناه هو أننا اتصلنا بسرعة بمزود الاستضافة وطلبنا من المسؤولين لديهم إصلاح المشكلة وإزالة صفحات التصيد الاحتيالي أيضًا. وبعد ساعات قليلة تمت إزالة صفحات التصيد الاحتيالي. الشريحة التالية رجاءً. ومن التهديدات الناشئة الأخرى التي لاحظناها أيضًا مع AMS، والتي كانت حديثة جدًا، هي مكتبة مفتوحة المصدر معرضة للخطر في عام 2024. لقد قمنا ببعض الفحوصات. كانت المشكلة بسبب قيام أحد الجهات الفاعلة المهددة بشراء اسم نطاق وشراء حساب GitHub لمكتبة مفتوحة المصدر شائعة. وبفضل هذا، تمكنوا من حقن تعليمات برمجية خبيثة في مكتبة، وبما أن المكتبة كانت مستخدمة على نطاق واسع، فقد كان لها تأثير واسع النطاق. وبسبب ذلك، لاحظنا أن هناك حوالي 40 نطاقًا SG. متأثرًا. لذا ما فعلناه هو أننا أخطرنا كل المسجلين حتى يتمكنوا من اتخاذ الإجراء اللازم. الشريحة التالية رجاءً.

فما هي التحديات التي واجهتنا عندما قمنا بتطوير هذا الجهد؟ أولًا، كان الأمر يتعلق بالتعليم والتوعية. لذلك، على الرغم من أن لدينا نظامًا لإخطار المسجلين، أدركنا أن بعض المسجلين لا يعرفون ماذا يفعلون بالمعلومات التي قدمناها لهم. بالإضافة إلى ذلك، هناك أوقات عندما ننظر إلى موفري الاستضافة، فإنهم أيضًا لا يدركون المشكلة ولا يعرفون أيضًا ما يجب فعله بالمعلومات التي قدمناها. ثانيًا، لاحظنا تأخيرًا في الحل. لذا أعتقد أن هذا يرجع إلى حد كبير إلى محاولة بعض المسجلين تحديد موفري الاستضافة الخاص بهم

وجزئيًا أيضًا لأن بعض موفري الاستضافة مترددون أيضًا في إصلاح المشكلة بسرعة لأن ذلك قد يكلف عملائهم الآخرين. وأخيرًا، هناك تحدي في بعض الأحيان يتمثل في إمكانية إزالة بعض المجالات ذات المخاطر العالية بسهولة. على سبيل المثال، كانت هناك حالة لاحظت فيها وجود نطاق يحتوي على غلاف ويب. بالنسبة لي، كشخص فني، أشعر أن الأمر كان خبيثًا جدًا. ولكن لأنها كانت ضحية، فلا يمكننا إغلاق الموقع. لذلك كان علينا إخطار الضحية وتعليمه كيفية إزالة الصفحة المفتوحة بسرعة. الشريحة التالية رجاءً. حسنًا، ما هو تأثير كل هذه الاستراتيجيات التي اتبعناها؟ أولًا، تمكنا من الحفاظ على مستوى منخفض من الانتهاك يبلغ حوالي خمس حالات مؤكدة شهريًا. ثانيًا، نجحنا في بناء الوعي المجتمعي. وبناءً على إشعارات البريد الإلكتروني التي يرسلها نظامنا، فقد نجحنا بطريقة ما في خلق وعي لدى جميع المستلمين لهذا البريد الإلكتروني. وبحلول ذلك الوقت، أصبحوا قادرين أيضًا على تعلم كيفية حماية أسماء النطاقات ومواقع الويب الخاصة بهم. وثالثًا، تمكنا من الحفاظ على الثقة في اسم النطاق sg.. لذلك، على الأقل في الوقت الحالي، تمكنا من ضمان بقاء نطاق sg. آمنًا وموثوقًا به. وأخيرًا، قمنا بزيادة ثقة الحكومة. وبفضل الجهود التي بذلناها في مجال اسم النطاق sg.، عهدت الحكومة إلى sg. أيضًا بتشغيل خدمة الرسائل النصية القصيرة وسجلات الهوية الخاصة بها، وهو ما يلعب دورًا رئيسيًا في مكافحة عمليات الاحتيال القائمة على الرسائل النصية القصيرة، والتي نعلم أنها مجال آخر من مجالات الجرائم المالية. شكرًا.

نيك وينبان-سميث رائع، شكرًا جزيلًا. لقد سجلنا بعض الأسئلة، ولكنني أرغب في الاطلاع على عرض بروس أولًا. سيكون هناك متسع من الوقت، على ما أعتقد، لأننا نسير على ما يرام، وبشكل مثالي. شكرًا للمتحدثين في الجدول الزمني. إذن لدينا العرض النهائي، لكن ابدأ بالتفكير في أسئلتك. إذا كنت في غرفة Zoom، فلا تتردد في إرسالها. سأحاول توزيعها بشكل عادل بين المشاركين عبر الإنترنت والمشاركين شخصيًا. وشكرًا جزيلًا مرة أخرى لـ مون على بقائه في منطقة زمنية غير اجتماعية من سنغافورة. الآن دورك يا بروس.

بروس تونكين شكرًا لك يا نيك. أحد الأشياء التي اعتقدت أنها مفيدة في هذه الجلسة، أعلم أننا في الجلسات السابقة تحدثنا عن التصيد الاحتيالي والبرامج الضارة، وأشار غابرييل إلى أن التصيد

الاحتيالي، على الأقل على المستوى الدولي، مرتفع للغاية. لقد ركزنا على ذلك خلال العامين الماضيين وربما شهدنا انخفاضًا بنسبة 10 في عدد مواقع التصيد الاحتيالي التي نراها في au.. في الغالب ما يتبقى هو ما نطلق عليه المواقع المخترقة، حيث يتم اختراق الموقع نفسه بصفحة تصيد، بدلًا من قيام شخص ما فعليًا بتسجيل اسم نطاق للتصيد. ويرجع ذلك إلى أن نوع العمليات التي نتبعها أثناء التسجيل تميل إلى إزالة معظم الأسماء التي تم إنشاؤها لأغراض التصيد الاحتيالي.

لكن ما ندركه هو أننا جزء من منظومة أوسع. ولإعطاء سياق في البيئة الأسترالية، فالاقتصاد الآن أصبح اقتصادًا رقميًا بالكامل تقريبًا. أعني، أنني أمضي أسابيع دون استخدام النقود. فكل المعاملات أصبحت إلكترونية. وفي حين أنه في الماضي، إذا تعرضت للاحتيال، فمن المحتمل أن يكون ذلك في أحد المطاعم المحلية، حيث يحاول شخص ما بيعك شيئًا ما. وإذا لم ينجح الأمر، فستعود إلى مقهى الشرب المحلي وتتحدث مع الشخص الذي باع لك هذا المنتج. في عالم الإنترنت، الشخص الذي يبيعك أو يخدعك لا يتواجد عادةً بالقرب منك. وفي السياق الأسترالي، فإنهم يعملون بالكامل تقريبًا من خارج أستراليا. وهذا يجعل الأمر صعبًا من وجهة نظر إنفاذ القانون. وهكذا يتحول التركيز أكثر. من الصعب جدًا القبض على الجاني الحقيقي. لكن ما يمكنك فعله هو محاولة تعطيل أنشطتهم على أمل أن ينتقلوا إلى مكان آخر. لذلك ركزت الحكومة على إطار عمل لمنع الاحتيال، والذي كان يقول إنه للتعامل مع القضايا، تحتاج حقًا إلى النظر إلى الجانب المالي، مثل كيفية تلقيهم للمدفوعات. يجب عليك النظر إلى الجانب المتعلق بالاتصالات. لذا فإن الرسائل النصية القصيرة التي يتم إرسالها إلى الهاتف، والتي أعتقد أن غابرييل قال إنها غالبًا ما تكون بداية لعملية احتيال. لذا لديك شركات الاتصالات، ومن ثم المنصات، والمنصات الرقمية مثل وسائل التواصل الاجتماعي، وفيسبوك، وما إلى ذلك. وعليك العمل بشكل تعاوني عبر هذه المنظومة. ولكل شخص في هذه المنظومة دور يلعبه. لدينا الآن مركز وطني لمكافحة الاحتيال. تمول الحكومة ذلك. وهذه نقطة تنسيق على المستوى الوطني لعمليات الاحتيال. والنشاط الآخر المثير للاهتمام في بيئتنا هو المقامرة التي تحظى بشعبية كبيرة في أستراليا. وأحد أنواع الاحتيال هو إنشاء موقع للمقامرة حيث يمكنك المراهنة على كرة القدم ولا تحصل على أموالك أبدًا عندما تفوز بالرهان لأنك تتعرض للاحتيال، في الأساس. لذا سأضع هذه الروابط هناك فقط حتى يتمكن الأشخاص من الوصول إلى بعض هذه المواقع. الانتقال إلى التالي.

أحد الأشياء التي لدينا في أستراليا هي بعض التعريفات التي اعتقدت أنها مفيدة للغاية. وبشكل عام، يجب أن تنطوي عملية الاحتيال على الخداع، وإذا نجحت، فإنها تؤدي إلى خسارة أو ضرر للمستهلك. وفي نهاية المطاف، فإن معلومات الاحتيال القابلة للتنفيذ هي المعلومات التي تمتلكها الشركة والتي تشير إلى نشاط احتيال محتمل يتعلق بأعمالها أو مرتبط بها. وأعتقد أن النقطة الأخيرة تتعلق حقًا بكوننا جزءًا من منظومة نحصل فيها على معلومات من عدد من المصادر، ويمكننا استخدام هذه المعلومات للإشارة إلى أنه قد تكون هناك عملية احتيال تحدث باستخدام اسم النطاق، ومن ثم يمكننا اتخاذ الإجراء. الشريحة التالية. وهذا هو الإطار الذي أنشأته الحكومة الأسترالية، والذي أعتقد أنه جيد جدًا، لأنه يقول بشكل أساسي أن هذه هي الخطوات المختلفة التي يجب على المنظمة ذات السمعة الطيبة والتي تعد جزءًا من المنظومة أن تتخذها. أحد هذه الأسباب هو أنه يجب أن يكون لديك عمليات استباقية للمساعدة في مكافحة عمليات الاحتيال. يجب عليك اتخاذ خطوات معقولة لمنع عمليات الاحتيال. بالنسبة لنا، الوقاية تكمن في أن نقوم بالتحقق المسبق في وقت التسجيل. نقوم بمراجعة التسجيلات الصادرة عن أمناء السجلات، ونقوم بمراجعة التسجيلات في وقت التجديد لمعرفة ما إذا كانت الشركات لم يتم إلغاء تسجيلها أو فقدت مكانتها في مجتمع الأعمال. نحن نكتشف ذلك، وهو ما يعني أننا بحاجة إلى اتخاذ خطوات معقولة للكشف عن النشاط، وأعتقد أن بعض ذلك قد ظهر هذا الأسبوع في بعض مناقشات وضع السياسات في GNSO، ولكن التسجيلات المجمعة هي مثال حيث يمكنك النظر إلى الأسماء حيث تم تسجيل الكثير من الأسماء في فترة قصيرة من الزمن. قد تكون هذه الأمور مشروعة، ولكن يجب عليك على الأقل اتخاذ الخطوات اللازمة لتتمكن من تحديدها والتحقيق فيها. التعطيل، وهو اتخاذ خطوات معقولة، حتى أتمكن من تحديد تلك الخطوات والتحقيق فيها. لذا، هناك مثال على ذلك إذا اكتشفت عملية احتيال، وأعتقد أنني سمعت بعض العروض هذا الأسبوع، حيث يقومون عادةً بذلك في دفعات من الأسماء، ونحن نرى ذلك. لذلك غالبًا ما تدرك أن هناك شخصًا أو شخصين يقومان بعملية احتيال في أي وقت معين، ومن المحتمل أن يقوموا بتسجيل مئات الأسماء، ثم تتوصل إلى النمط الذي يتبعونه. وبمجرد أن تتوصل إلى نمطهم، يمكنك التخلص من مجموعة أسمائهم الحالية. ثم عليك أن تراقب الأمر لعدة أسابيع، لأنهم ما زالوا لا يفهمون الصورة بشكل كامل، وما زالوا يواصلون تسجيل أسماء جديدة باستخدام نفس عملية الاحتيال السابقة. وبعد ذلك، بمجرد الاستمرار في إغلاقها أو إيقاف تسجيلها، فإنها تنتقل في النهاية إلى شخص آخر في الغرفة، أو رمز دولة آخر أو نطاق المستوى الأعلى. وهذا هو السبب أيضًا وراء ضرورة مشاركة

المعلومات بشكل أكبر، لأنني أشك في أنه بمجرد أن نتعامل مع شخص ما، فإنه ينتقل إلى شخص آخر في هذه الغرفة. ثم الرد بشكل واضح، والرد على التقارير. والجزء الأخير الذي لا نزال نحاول العمل عليه هو كيفية الإبلاغ عما نراه والذي يمكن للآخرين في هذه الغرفة اتخاذ إجراءات بشأنه. الشريحة التالية.

أردنا فقط تسليط الضوء على النوعين الرئيسيين من مشكلات أسماء النطاقات التي نواجهها. وهناك فئة واحدة نشير إليها بالخبيثة، وهي الفئة التي يستخدم فيها المسجل عادةً معلومات كاذبة. ورغم أن لدينا خطوات للتحقق، إذا كنت تستخدم معلومات مسروقة، أو تستخدم رخصة قيادة مسروقة لشخص ما، أو جواز سفر مسروق، أو معلومات تجارية مسروقة، فإن هذا يجتاز معظم عمليات التحقق المسبقة. لذلك نجد أن المحتالين أصبحوا أكثر تطورًا وسرقوا المعلومات. لقد قاموا باختراق شخص ما. لقد حصلت على معلومات من هذا الاختراق من شركة أخرى، واستخدمها لتسجيل أسماء النطاقات. الشيء الوحيد الذي يصب في صالحنا هو أن لدينا متطلب الوجود الأسترالي. أعتقد أنني سمعت cn. الصين اليوم، وسنغافورة، على ما أعتقد، العرض السابق. لأن لديهم قواعد تنص على أن اسم النطاق يجب أن يكون مرتبطًا بالدولة بطريقة ما، ويمكن استخدام ذلك كأساس للكشف عن المعلومات الكاذبة. لذلك عندما نرى اسمًا يتم استخدامه، على سبيل المثال، في عملية احتيال مالية، فإننا لا نزيل اسم النطاق لأن هناك عملية احتيال مالية. لقد قمنا بإزالة اسم النطاق لأنهم استخدموا معلومات خاطئة. وبذلك يمكننا أن نأخذ التقارير من وكالة إنفاذ القانون. لا يتعين عليهم إصدار أمر من المحكمة. إنهم يقولون فقط، إليك اسم النطاق الذي تعتقد أننا قد نشارك فيه في عملية احتيال. وإذا نظرنا إليه ورأينا أنه يحتوي على معلومات خاطئة، فسوف نزيله. ونحن نقوم بإزالته لأنهم انتهكوا قواعد التسجيل لدينا، وليس بسبب القوانين الأخرى التي ربما انتهكوها.

والفئة الثانية التي نراها كثيرًا في au. هي المواقع المخترقة. وتستخدم العديد من مواقع الويب التجارية نوعًا من حلول مواقع الويب الجاهزة. بعض هذه الحلول لديها آليات تمكنك من كتابة مراجعات للمنتجات وتحميل المحتوى على موقع الويب، وهو خطأ كبير لأن المحتالين يقومون بتحميل المحتوى على موقع الويب ويضعون روابط على تلك المواقع لمواقع ضارة أو محتوى ضار. يتم اختراق مواقع الويب، وهذا يعني أنهم يستخدمون إصدارًا غير مُرقّع، عادةً WordPress. ولذلك في مثل هذه المواقف، لا نقوم بإزالة اسم النطاق لأننا لا نريد إغلاق العمل. نقوم بإخطار أمين السجل، ويقومون بالاتصال بالمسجل.

وعادة ما يفاجأ المسجلون للغاية عندما يكتشفون أنهم يستضيفون بعض المحتوى السيئ من نوع ما، وعادة ما يكونون استباقيين للغاية في معالجته. لا تزال هناك مشكلة تثقيف المستخدم لأنه في كثير من الأحيان عندما يتم الاتصال بالمسجل، فإنه لا يعرف حتى من هي شركة الاستضافة الخاصة به، والشخص الذي قام ببناء الموقع قد غادر منذ بضع سنوات. وهذا غالبًا ما يستغرق وقتًا طويلًا ونحن نساعدهم على فهم المنظومة، ومن يحتاجون إلى التحدث إليه، والعمل معهم لإصلاح الموقع الإلكتروني بدلًا من إزالته. الشريحة التالية.

لذا، هذا هو ما استخدمته للتو من إطار عمل مثل إطار الاحتيال الأسترالي، وهو على مستوى الحوكمة، حيث نتتبع جميع تقاريرنا ونبلغها إلى مجلس إدارتنا. نواصل تشديد إجراءات التحقق لدينا، لأنها إحدى الإجراءات الوقائية التي يمكننا اتخاذها. نكتشف أي اسم، ثم نبحث عنه، بعد تسجيله، ونتحقق منه. ونبحث عن الأنماط المرتبطة بالاحتيال. على سبيل المثال، بالنسبة لمواقع المقامرة، قد نقوم بإجراء عمليات بحث على Google عن محتوى ذي صلة والعثور على نطاقات أخرى تناسب هذا النمط والبحث عن أنواع مختلفة من العلامات، إذا أردت، في بيانات التسجيل وإزالة دفعات من الأسماء. وهذا النوع من الاضطراب يؤدي إلى البحث بشكل استباقي عن النطاقات ذات الصلة. إذا كان هناك نطاق واحد تم الإبلاغ عنه من خلال عملية احتيال، فمن المحتمل أن يكون لديك بالفعل مئات النطاقات في السجل، ويتم العثور عليها وإغلاقها. نحاول أن نكون متجاوبين ونعمل مع وكالات إنفاذ القانون ونشجعهم على الإبلاغ عن الأشياء لنا. ولكنني أود أن أقول إن المعلومات التي نحصل عليها من جهات إنفاذ القانون ربما تكون أقل بنسبة 1%، وربما أقل من ذلك بكثير. لذلك في الغالب نحن نشترك في عدد من موجزات المعلومات وموجزات التهديدات الذكية، وهذا هو المصدر الذي نحصل منه على معظم معلوماتنا الاستخباراتية. لكننا نستجيب لسلطات إنفاذ القانون حسب الحاجة. والجزء الأخير، وهو ما أشجعنا على البدء في التفكير فيه كمجتمع، هو كيف نشارك المعلومات؟ وهذا أمر صعب لأنك لا تريد مشاركة المعلومات التي تخضع لقانون الخصوصية. ولكن كلما تمكنا من مشاركة المزيد من المعلومات، وكما قلت، أعتقد أنه عندما نكتشف أشياء غير عادية، فمن المحتمل أن يحدث ذلك بالتأكيد في نطاقات gTLD الرئيسية الأخرى ورموز البلدان أيضًا. وبالتأكيد ندعم العمل الذي تقوم به مؤسسة البنية التحتية للإنترنت، والذي أعتقد أنه كان يعمل عليه فريق كيث، ولكن هذا النوع من التنسيق بين أمناء السجلات وشركات الاستضافة. لذا فإن

الأمر يتجاوز مجرد نطاق ضار، بل إنه ينظر إلى كيفية تعطيل الجهات الفاعلة السيئة بشكل جماعي. وأعود إليك مرة أخرى، نيك.

نيك وينبان-سميث شكرا جزيلا لك، بروس. أعتقد أنه من خلال العروض المختلفة، هناك الكثير مما يجب توضيحه حول حقيقة أن هذه ظاهرة ضخمة النطاق والتكلفة بالنسبة لمواطنينا الذين نحن هنا للدفاع عن مصالحهم، وكذلك التأثير على عمليات التسجيل من المنظورين السنغافوري والأسترالي، وكم من الوقت والجهد يحتاجان إلى بذله في هذا الصدد. لكن هذا الوقت والجهد، في رأيي، لا يزال يشكل جزءًا صغيرًا للغاية من حيث تكلفة الخسائر التي لا تزال مستمرة بالنسبة للمستهلكين. سمعنا أن الثقة والسمعة تشكلان مشكلة كبيرة. وأعتقد أنه مع تزايد التحول الرقمي للأمور، أصبح من الممكن معالجة هذا النوع من القضايا حتى يتمكن الناس، بثقة، من معرفة أن من يتعاملون معه هو في الواقع من يعتقدون أنهم يتعاملون معه عندما يتعلق الأمر بالسلع والخدمات، والاستثمار بطبيعته لا يجب أن يتم عبر الإنترنت أيضًا. لذا أعلم أن لدينا بعض الأسئلة بالفعل، وأعتقد أن أولغا كانت الأولى في قائمة الانتظار. لقد حصلنا على ربع ساعة تقريبًا. الآن الدور عليكِ يا أولغا، أما بالنسبة للجميع، فعليهم أن يرفعوا أيديهم في الغرفة. أستطيع رؤية هيلدا بعد ذلك. وإذا كنت في Zoom، ارفع يدك في Zoom.

أولغا كافالي شكرًا لك يا نيك. شكرا جزيلا على العروض. لدي سؤال لممثل مكتب التحقيقات الفيدرالي. لقد نسيت اسمك. عذرًا على ذلك. وما هو حجم الخسائر التي ذكرتها في عرضك، هل هو شيء تم تقديره من قبل الضحايا أم أن لديك طريقة لحسابه بناءً على الضرر الذي لحق بالضحايا؟ كنت أتساءل عما إذا كان بإمكانك شرح ذلك قليلًا.

غابرييل أندروز بالتأكيد. يسعدني ذلك. لكن نعم، معظم أرقام الخسائر هي أرقام تم الإبلاغ عنها ذاتيًا. لذا، بحلول الوقت الذي تتقدم فيه القضايا ونتحرك نحو نوع ما من الملاحقة القضائية، من الواضح أننا سنضطر إلى التحقق من ذلك من أجل المضي قدمًا في أي نوع من المحاكمة. لكن عندما نقوم فقط بجمع الإحصائيات، فإننا نميل إلى جمع الخسائر التي تقدم بها الضحايا.

ولكن في بعض الأحيان، بصراحة، قد يرغب الضحية في المبالغة في الخسارة. أنت تتحدث عن أشياء مثل التهديدات أو الخسارة لصورة علامتهم التجارية وسمعتهم. ونحن لا ندرج أي شيء من ذلك. لكن هناك أشياء ملموسة للغاية، مثل تعرضنا لهجوم فدية وأُجبرنا على دفع 5 ملايين دولار للوصول إلى شبكتنا مرة أخرى. من السهل جدًا التعبير عن الخسارة. أو كان لدينا تحويل بنكي خرج واعتقدنا أنه كان يدفع لأحد البائعين لدينا. اتضح أن أحد الأشخاص هو الذي اخترق البريد الإلكتروني وخدعنا. إنها سهلة التعبير عنها. ومن هنا جاءت تلك الأرقام، أو الجزء الأكبر منها.

نيك وينبان-سميث شكرًا. هل يجب علينا نقل الشريحة والانتقال إلى سؤال هيلدا التالي؟

هيلدا ثونيم شكرًا. أنا هيلدا ثونيم من السجل النرويجي. لدي في الواقع سؤالان، ولكنني سأبدأ بسؤال موجه إلى مكتب التحقيقات الفيدرالي. على الأقل يبدو أن الأبحاث الأخيرة التي رأيتها تشير إلى أن حوالي 80% من عمليات التصيد تأتي الآن، أنا فقط أتساءل، عندما تتعامل مع حالة، ترى هذا النمط، وأفترض، هل هناك فرق في كيفية التعامل مع، ما هو موقع ويب مخترق، أو نطاق مخترق؟ لأن حينها سيكون الشخص الذي يقف خلف النطاق هو الضحية فعليا. وأعتقد أنه يتعين عليك عدم الاتصال بالسجل والطلب منهم إزالة اسم النطاق. نأمل ذلك.

غابرييل أندروز إنه سؤال مهم جدًا. نعم، أعتقد أنك على حق تمامًا في أن الاستجابة للحقائق والظروف التي أمامك في أي وقت معين سوف تتغير، أليس كذلك؟ وما هو الرد المعقول سوف يتغير نتيجة لذلك. بالنسبة لنقطتك، إذا أردنا بشكل عام، فإن أحد أول الأشياء التي تحاول القيام بها عندما تسمع لأول مرة عن جريمة تم الإبلاغ عنها لك هو معرفة أين يتوقف الرجل السيئ وأين ينتهي، أليس كذلك؟ أو مثل حيث يتم التحكم في البنية التحتية فعليًا بواسطة الرجل السيئ، أو ربما تكون شركة مشروعة وهو مجرد عميل لها. وقد تستغرق هذه الأمور بعض الوقت لمعرفة مكان حدوثها. وبالنسبة لنقطتك، إذا كانوا يستخدمون موقعًا إلكترونيًا لشخص مخترق، فقد يستغرق الأمر بعض الوقت لمعرفة ذلك أيضًا. لكن عندما

نحاول التخفيف من الضرر، فأنت على حق تمامًا في أن الأمر سيكون أكثر منطقية إذا تمكنت من تحديد أن النطاق تم تسجيله بشكل ضار، فربما تطلب من أمين سجل أو مشغل سجل اتخاذ نوع من الإزالة له. لكن هذا ليس على الإطلاق الخيار المناسب في حالة تعرض الموقع للخطر. لكن الآن لديك ضحية أخرى لإضافتها إلى قائمتك، أليس كذلك؟ وقد يكون من الضروري أن يكونوا جزءًا محتملًا من محاكمتك في المستقبل. لأنه في الولايات المتحدة، على الأقل، يعد الوصول غير المصرح به إلى نظام كمبيوتر محمي انتهاكًا للقانون الأمريكي. وهكذا وقعت جريمة أخرى هناك.

هيلدا ثونيم

أجل. ولمتابعة AUDA، لأنني أحب حقًا أن أرى أنك تفكر في كيفية التعامل مع المخاطر، والتي من المحتمل أن تكون كمية كبيرة من عمليات التصيد والاحتيال. ولكن ما هي تجربتك عندما تحاول الاتصال بشخص ما وإخباره بأن موقعه على الويب قد تعرض للاختراق؟ لأنني أعلم أنه باعتبارنا سجلًا، نحن غير مرئيين للغاية. ومحاولتي الاتصال بشخص ما لأقول له إن جريمة ارتكبت لمحاولة القيام بشيء ما، يُنظر إليها على أنها عملية احتيال. لذا فإنني أفضّل بالتأكيد أن تكون هذه الجهة هي الشرطة أو هيئة الشهادات أو شخص يعرفه الناس بدلًا من هذه الشركة الغريبة التي تدّعي أنها تدير الإنترنت في النرويج. ويريدون منك أن تفعل شيئًا يتعلق بموقعك الإلكتروني. ويجب عليك القيام بذلك بسرعة كبيرة جدًا لأن الضرر يحدث. وأنا أضع علامة على كل، كما تعلمون، مربعات الاحتيال هنا. أنت كذلك.

غابرييل أندروز

نعم، حسنًا. نعم، نحن جميعا نتفق. أستطيع أن أرى هذا. نعم، وكأننا جميعًا في اتفاق عنيف. ولكنك على حق تمامًا. هناك تحديات كبيرة في إخطار الضحايا. وفي الماضي، عندما تعاونا مع القطاع الخاص في عمليات إزالة كبيرة، وكان من الممكن أن يشمل هذا التعاون شركات تقنية كبيرة للغاية، أو شركات البنية التحتية للإنترنت، أو مقدمي خدمات الإنترنت، أو شركات مثل Microsoft. يمكن أن يكون الأمر بمثابة محاولة موازنة بين مدى رغبتك في الاعتماد على القطاع الخاص في الإخطار أو مدى منطقية قيام جهات إنفاذ القانون بذلك. وكانت هناك مناسبات في الماضي حيث اعتقدنا أنه من المعقول أن يقوم مزودو خدمة الإنترنت بإخطار عملائهم، وأعتقد أن هذا ربما حدث في حالات تسميم ذاكرة التخزين

المؤقت لنظام أسماء النطاقات. أحاول أن أتذكر أين تعلمت ذلك. ولكن ما سمعته من وكلاء القضية الذين عملوا في ذلك الوقت، ومقدمي خدمات الإنترنت الذين عملوا معهم، هو أن عملاء مقدمي خدمات الإنترنت شعروا في الواقع بغضب شديد تجاه مقدمي خدمات الإنترنت لأنهم بدأوا في إلقاء اللوم عليهم بسبب الاختراق، على الرغم من أنهم لم يكن لهم أي علاقة به. لقد كانوا يحاولون فقط اتخاذ هذا الإجراء المسؤول. لذا أعتقد أن جهات إنفاذ القانون تدرك أن هناك دورًا يجب أن نلعبه للمساعدة حقًا في عمليات إخطار الضحايا. قد يختلف الأمر من بلد إلى آخر، ولكن هذا جزء مطلق من الأمر، وبالحديث عن نفسي فقط، وليس عن وكالتي، أرى هذا كجزء من دوري للمساعدة. لكن هذا يشكل تحديًا وليس من السهل حله، لسوء الحظ.

نيك وينبان-سميث

شكرًا. لقد حصلت على بيير ومن ثم ريان سيمبوليك. ولكن أولًا وقبل كل شيء، هيلدا، أو أي شخص آخر، هل تدعمين قيام السجل بتقديم متطلبات قانونية للمسجلين للحفاظ فعليًا على النظافة الأمنية الأساسية على مواقعهم على الإنترنت؟ ولكي يكون هذا في الواقع شيئًا يجب على السجل...

هيلدا ثونيم

لا، لأنني لا أطلب منهم أن يكون لديهم موقع على شبكة الإنترنت. إنهم يشترون اسم نطاق، ويشترون حق استخدامه ليكون موجودًا في قاعدة البيانات، ليكون له ترجمة عندما يقوم شخص ما بإدخال اسم النطاق هذا للعثور على عنوان IP. ليس من الضروري أن يكون لديهم موقع على شبكة الإنترنت. ليس من الضروري أن يكون لديهم بريد إلكتروني. هذه هي الخدمات التي اختاروها. يشترون من شيء آخر. أنا لا أقوم بتسليمهم. وهم المسؤولون الوحيدون، وفقًا لقانون الاتصالات الإلكترونية في النرويج، عن استخدام اسم النطاق الخاص بهم. لذا فإن إدراجي في العقد الذي ينص على ضرورة قيامهم بأشياء معينة لا أكون جزءًا من تقديمها سيكون بمثابة إدراجي في العقد أيضًا، حيث أكون سخيفًا، لإثبات وجهة نظري. لكن عليك أن تنظر في كلا الاتجاهين عندما تعبر الطريق ولا تركن سيارتك في مكان لا يسمح فيه بالركن. إنها جريمة، ولكن ليس لها علاقة بي. لذا لا، لن أؤيد ذلك في عقدنا.

نيك وينبان-سميث شكرًا. بيير؟

بيير شكرًا جزيلاً لك، نيك. وشكرا لكم على هذه الجلسة المثيرة للاهتمام للغاية، واللجنة المتنوعة للغاية. لذا أولًا وقبل كل شيء، أردت أن أقول، كالعادة، إنني أتفق تمامًا مع NO. ومع هيلدا. هذا لا يعني أننا لا يجب أن نتصرف عندما نرى أن هناك مشكلة على الموقع. ولكن الأمر مختلف. أعني، إذا وضعت في عقد ما شيئًا مثل أنه يتعين عليك التأكد من الحفاظ على أمان موقع الويب الخاص بك، فإن السؤال الذي سأطرحه بعد ذلك هو، كيف يمكنني فرض عقدي الخاص؟ كيف يمكنني التأكد من أن المسجل قام بتصحيح موقعه الإلكتروني؟ لذا فأنا لا أحب أن أضع في العقد شيئًا لا أستطيع فرضه.

لكن السؤال الذي أردت أن أطرحه على المشاركين، وربما بشكل خاص على المشاركين من مكتب التحقيقات الفيدرالي، هو ما إذا كان بإمكانكم مشاركة المعلومات حول نوع المناقشات التي تجريها مع شركات الهاتف. لأننا نتحدث عن البيانات الموجودة في Waze. معظم عمليات الاحتيال التي أتلقاها، ربما تكون خاصة بفرنسا، أتلقاها عبر رسالة نصية قصيرة على هاتفي الآيفون. وهي ليست أرقامًا مخفية. إنها أرقام حقيقية. وأعتقد أن الأشخاص الذين يرسلون لي هذا النوع من الأشياء لم يعطوا عنوانهم الحقيقي أو اسمهم الحقيقي لمشغل الهاتف. وإلا فسيكون من السهل جدًا القبض عليهم. لذا لا أعرف كيف يعمل. ولكنني أعتقد أننا نشهد المزيد والمزيد من الطلبات من البنوك أو مقدمي خدمات الإنترنت أو مشغلي الهاتف لإجراء التحقق المطلوب منهم في عالم الاتصالات. ويبدو أنه لا يعمل أيضًا. لذلك أود أن أعرف كيف تتعامل مع ذلك؟ شكرًا.

غابرييل أندروز سأعترف بأن هذا سؤال عادل. يجب علي أن أعتذر. ليس لدي إجابة جيدة لك. أنا شخصيًا لم أتحدث إلى مشغلي شركات الاتصالات في أي وقت في الآونة الأخيرة. لذا سأضطر إلى تجنب ذلك. ومع ذلك، أود أن أقول إنه على مستوى الطيف، أعتقد أن هناك اعترافًا متزايدًا بأننا سنواجه مجتمعًا به الكثير من التحديات المحيطة بمصادقة الهوية وحتى المصادقة على أنك شخص حقيقي في الحياة الواقعية في السنوات القادمة. مع ملاحظة التقدم، سأغير

الموضوع قليلًا هنا، ولكن سألاحظ كيف أصبحت الأدوات مثل الذكاء الاصطناعي ناجحة بشكل متزايد في انتحال شخصيات الأشخاص. والتحديات التي تواجهك هي معرفة أنه عندما تتحدث إلى أي شخص عبر الإنترنت، كيف يمكنك أن تثق بأي شيء بعد الآن؟ وأعتقد أن هذه هي التحديات التي يتعين علينا مواجهتها، لكن ليس لدي حلول. ولسوء الحظ، فيما يتعلق بشركات الاتصالات، نعم، هناك الكثير مما يمكن قوله. أنا لست الشخص المناسب لقول ذلك.

بيير شكرًا. أردت فقط أن أضيف أنه إذا فعلت ذلك، إذا سألت هذا السؤال، فأنا أفهم تمامًا أنك لست مستعدًا لذلك. لكنها أيضًا طريقة للقول بأن أرقام الهواتف هي معرّفات. لا أحد يرتكب الخطأ. لا أحد يعتقد أن رقم الهاتف هو محتوى. حسنًا. أسماء النطاقات هي معرفات. إذن هناك رابط حقيقي بين الأمرين. أعتقد أننا يجب أن نحاول حقًا معرفة كيفية أدائهم في صناعة الاتصالات، لأننا نتحدث دائمًا عن المعرفات وليس المحتوى.

نيك وينبان-سميث شكرًا. سأنتقل سريعًا إلى بروس، ثم إلى كيث، وبعد ذلك سننتقل إلى سؤال بريان.

بروس تونكين نعم، كنت سأقول فقط أن هذا هو بالضبط ما تحاول الحكومة الأسترالية التعامل معه، لأن كل مجموعة تقول إنها مشكلة شخص آخر، ويقولون إن عليك في الواقع دمج الشيء، لأنه عادة ما يكون عبارة عن رسالة نصية قصيرة. في الواقع، هناك حساب مصرفي يتم الدفع إليه في مكان ما، وهو المكان الذي تذهب إليه الأموال، وعادةً ما يكون هناك اسم نطاق كرابط داخل رسالة SMS، لذا فهو مزيج. ما أراه مثيرا للاهتمام، على سبيل المثال، فيما يتعلق بالهاتف، لأنه في أستراليا يعتمد في الغالب على الرسائل النصية القصيرة أيضًا، ولكن الآن يمكنك الإبلاغ عنها باعتبارها عملية احتيال. عندما تقوم بحذفه يقول هل هذه عملية احتيال؟ أنت تقول نعم فقط، ولكن أين تذهب تلك التقارير؟ أعتقد أنهم يحاولون ربط كل النقاط، وهذا بالتأكيد ما كنا نحاول القيام به في أستراليا، حيث بدأوا في إنشاء سجلات لأرقام الهواتف التي تسبب مشكلة، ثم لا يقومون بتوجيهها من شركة اتصالات إلى أخرى.

كيث درازيك شكرًا جزيلًا لك على هذا السؤال، وأود فقط أن أبني عليه. منتدى البنية التحتية للإنترنت، رؤيتنا أثناء بناء هذا المنتدى وتطوره هي أن ندرج شركات الاتصالات عندما نتعامل مع الأضرار عبر الإنترنت المتعلقة بهجمات الرسائل النصية القصيرة، وهجمات الرسائل النصية القصيرة، لتشمل معالجات الدفع عندما نبدأ في الحديث عن الاحتيال المالي. لذا أعتقد أن التوقع هو أنه بما أن لدينا سجلات وأمناء سجلات ومضيفين على الويب وشبكات توصيل المحتوى، فإننا سنستمر في إضافة لاعبين إضافيين لديهم أدوار في التخفيف من هذه الأضرار. نحن جميعًا لدينا مجالات مختلفة من المسؤولية والقدرات التقنية، ولكن التنسيق مهم حقًا، وهذا هو أحد أهداف الجهود. شكرًا.

نيك وينبان-سميث شكراً لك يا كيث. ننتقل الآن إلى بريان. أعتقد أن هذا ربما يكون السؤال الأخير. لدينا بضعة شرائح أخرى، وبعد ذلك سوف نختتم. شكرًا جزيلًا.

برايان سيمبوليك مرحبًا، أنا بريان سيمبوليك من سجل المصلحة العامة. غابي، هذا ينبغي أن يكون سؤالا سريعا. بخصوص تقرير الجرائم على الإنترنت أو تقرير الجرائم عبر الإنترنت، سؤال واحد كنت أتوقع متابعته. هل هذه الجرائم مرتبطة فقط بأسماء النطاقات، أم أنها تشمل منصات التواصل الاجتماعي؟

غابرييل أندروز وهذا يشمل أي شيء يتم الإبلاغ عنه لنا باعتباره جريمة متعلقة بالإنترنت، أليس كذلك؟ لذا هناك مجموعة من الفئات هناك، وأنا أواجه صعوبة في كل مرة أحضر فيها هذه البيانات إلى ICANN لمحاولة جعلها ذات صلة بك قدر الإمكان. ولهذا السبب أحاول تسليط الضوء على مواطن التداخل مع نظام أسماء النطاقات وحتى على مدى رغبتنا كمحققين في استخدام الأدوات التي تتطرق إلى نظام أسماء النطاقات. لكن لا، إنه يتجاوز ذلك بكثير وربما يكون أكثر بكثير مما أستطيع التحدث عنه.

برايان سيمبوليك باختصار، هل كان لديك أي فكرة عن حجم عمليات الاحتيال على وسائل التواصل الاجتماعي مقارنة بتلك المرتبطة بأسماء النطاقات؟

غابرييل أندروز أتمنى أن أفعل ذلك، ولكنني لا أعلم أننا نصنفه إلى هذه الدرجة من الإخلاص. أعتقد أنهم بالفعل يضعون الأشياء في مجموعات أكبر مثل التصيد الاحتيالي، لكنني لا أعرف ما إذا كانوا ينقسمون إلى التصيد الاحتيالي استنادًا إلى التصيد عبر الرسائل النصية القصيرة مقابل WhatsApp وتطبيقات الدردشة مقابل النطاقات. أو حتى إذا كان هناك تصيد على الرسائل النصية القصيرة، فهل تضمن ذلك أيضًا اسم نطاق ضمنها؟ هذه كلها أسئلة ذات صلة. لا أعتقد أن لدينا هذه التفاصيل الدقيقة في البيانات.

برايان سيمبوليك سيكون من الرائع لو تمكنت في مرحلة ما، وخاصة مع عرض هذه البيانات أمام مجتمع DNS، من تحليل هذه البيانات، لأن إحساسي هو أن هذا الأمر من المرجح أن يحدث على منصات التواصل الاجتماعي أكثر من حدوثه بواسطة DNS.

غابرييل أندروز أوافق على أنه سيكون من الرائع الحصول على قدر أكبر من الدقة. سنعمل على تحقيق ذلك مع مرور الوقت.

نيك وينبان-سميث شكرًا جزيلًا. هذه منطقة رائعة. يمكنك أن تقول أنها معقدة. أعتقد أن أحد أهداف عقد مثل هذه الجلسات هو التحدث عبر مختلف الجهات الفاعلة ووجهات النظر المختلفة، لأن فهم السياق الذي يتم فيه تقديم بعض هذه الشخصيات، أعتقد أنه من المهم للغاية بالنسبة لنا كمشغلين فنيين للبنية التحتية أن نرى أننا نفعل ذلك بقدر ما نستطيع لمنع هذا النوع من الجرائم، ولكن أيضًا لفهم أين ربما توجد أماكن أخرى لا تقف حقًا والتعامل معها. وعلى وجه الخصوص، تحدثنا إلى أصدقائنا الحكوميين والجهات التنظيمية للسياسات، ثم فهمنا

السياق ومدى تعقيده عبر الكثير من المنصات المختلفة ومتجهات الهجوم، وأن هذا ليس سوى عنصر واحد منه، وهناك مجالات أخرى أيضًا، وأعتقد أن هذا جزء مثير للاهتمام للغاية من المناقشة. لذا سنقوم بنقل هذا الأمر بسرعة. سوف نفعل الاستطلاع مرة أخرى. دعونا نلقي نظرة الآن على سؤال الاستطلاع. سأتوقف عند هذا الحد لأنها نهاية الجلسة، ولكن بشكل أساسي تغيرت الأمور قليلًا، ولكن ليس كثيرًا بمعنى أن هناك بعض المجالات التي لا يشعر فيها الناس أن سجلاتهم مستعدة بشكل جيد بما يكفي للكشف عن الانتهاكات، وربما ليست مستعدة بشكل جيد كما يرغبون في أن يكونوا من حيث القدرة على الاستجابة للجرائم المالية. سمعنا عن تعقيدات المواقع الإلكترونية المخترقة. وأخيرًا، أود أن أقدم تصفيقًا حارًا، حقًا، لأعضاء اللجنة الرائعين. لذا شكرًا جزيلًا لكم. تتضمن مجموعة الشرائح بعض الموارد للمكتب التي يمكننا الرجوع إليها، ثم هناك استطلاع نهائي لتقييم الجلسة. لذا سأترك لكم القيام بذلك والاستمتاع بوقت استراحة القهوة الخاص بك. شكرًا جزيلاً لكم جميعًا. شكرًا.

[انتهاء تدوين النص]