AR

جوهانسبرغ– جلسة رقم 2 لبناء القدرات لمنظومة من منظومات المجتمع الشامل لعموم المستخدمين التابعة لمنظمة AFRALO في أفريقيا
الثلاثاء، 27 يونيو 2017 – من الساعة 08:00 ص إلى الساعة 09:00 ص بتوقيت جوهانسبرغ
ICANN59 | جوهانسبرغ، جنوب أفريقيا

شخص غير محدد: إنها جلسة رقم 2 لبناء القدرات لمنظومة من منظومات المجتمع الشامل لعموم المستخدمين التابعة لمنظمة AFRALO في أفريقيا، بتاريخ 27 يونيو 2017، من الساعة 08:00 ص إلى الساعة 09:00 ص في القاعة الرئيسية 4.

عزيز هلالي: أهلاً ومرحبًا بكم في الجلسة الثانية، جلسة بناء القدرة التي ننظمها كل يوم في الساعة 08:00 صباحًا. سوف يكون موضوعنا اليوم التحديات، أي التحديات الأمنية التي تؤثر على المسجلين والمستخدمين النهائيين. وهو موضوع مهم للغاية. وهذا هو السبب في عقد هذه الجلسة الثانية للحديث حول هذا الموضوع ويسرني اليوم أن أعرض لكم اثنين من المتحدثين، وأود أن أشكرهم كثيرًا على حضورهم هذا الصباح للتحدث إلينا.

أما ستيف تشينغ الذي يجلس على يساري فهو مدير التنمية الاستشارية للجنة الاستشارية للأمن والاستقرار واللجنة الاستشارية لنظام خادم الجذر، ولدينا السيد ديفيد بيستشيللو، وهو نائب الرئيس في قسم تنسيق الأمن وتقنية الاتصالات والمعلومات. وأود أن أشكرهم كثيرًا وأعطي الكلمة لستيف تشينغ. يمكنك البدء الآن، ستيف.

ستيف تشينغ: شكرًا لك سيدي الرئيس، ونائب الرئيس. وإنه لمن دواعي سروري أن أكون معكم اليوم. أُدعى ستيف. وهذه هي المرة الثالثة لي في أفريقيا، وفي كل مرة آتي إلى هنا، أشعر بحرارة الترحيب كما لو كنت في وطني، حتى على متن الطائرة في جنوب أفريقيا، شعرت بذلك. وإنه لمن الرائع حقًا وجودي بينكم.

وكما ذكرت، اسمي هو ستيف. وإنني أعمل في قسم السياسة. ويدعم فريقنا وضع استشاريات لجنة الأمن والاستقرار، وكذلك اللجنة الاستشارية لنظام خادم الجذر.

ويجلس إلى يساري، زميل سابق لي، أود أن تقدم نفسك، ديف. ومعكم الآن ديف.

ديفيد بيستشيللو: طاب صباحكم. ديف بيستللو. وأعمل نائبًا لرئيس قسم تنسيق الأمن وتقنية الاتصالات والمعلومات في ICANN. وأعمل في المقابل مسؤولاً فنيًا رئيسيًا وأنا جزء من فريق الأمن والاستقرار والمرونة.

ستيف تشينغ: شكرًا. بالتالي، نريد أن نجعل القسم اليوم أكثر تفاعلاً ونريد أيضًا أن نركز أكثر على المسجل ونتناول بعض الشيء عن المستخدم النهائي. غير أنني أرغب في بدء وضع سياق وإطار عمل. فعندما نفكر في التهديدات الأمنية أو المسائل الأمنية، فيمكن تقسيم هذه إلى ثلاث فئات على نحو كبير. أما الفئة الأولى فسيطلق عليها اسم هجوم مادي. وهذه هي أنواع الهجمات التي تهاجم بالفعل البنية التحتية، وتهاجم البنية التحتية للاتصالات، والسقف، وقطع الكابلات. بالتالي فإننا لدينا ما يسمى بالهجوم المادي.

أما الجزء الثاني من الهجوم فهو ما نطلق عليه هجوم مفْصلي. وذلك يهاجم كيفية تشغيل الأعمال والبروتوكولات لهذه الأنظمة التي تهاجم نقاط الضعف في هذه البروتوكولات نفسها. وقد رأيتم هذه الهجمات، على سبيل المثال، كان آخرها، برمجيات الدفع القسري للفدية، حيث إنه يستخدم مستغل نظام Windows، ويستخدم ذلك لإدخال برمجيات الدفع القسري للفدية على أجهزة الكمبيوتر للأشخاص، ويستخدم ذلك كوسيلة للحصول على المال.

وهناك مثال آخر للهجوم المفصلي هو هجمات حجب الخدمة، حيث يتظاهر المهاجم الضار بمحاولة اجتياح المرور الشرعي ومثال على ذلك نظام اسم النطاق، حيث تحصل على رد قبل [غير مسموع] إعادة الرد، بالتالي فإنك كمهاجم تصبح المتحكم في مجريات الأمور.

لذلك، تلك هي الطرق التي يهاجم بها الهجوم المفْصلي البروتوكولات، وتصميم البروتوكولات، ونقاط الضعف في النظام. بالتالي، فإننا لدينا ما يسمى بالهجوم المفْصلي.

أما الفئة الثانية من الهجوم فهي ما نطلق عليها هجوم دلالي. ويهاجم هذا النوع من الهجوم كيفية تعيين الأشخاص للمعاني بالنسبة للواجهة التي يتفاعلون بها. ومن الأمثلة الأكثر شيوعًا لهذا الهجوم هو التصيد أو التصيد بالرمح، حيث إنه في هذا السياق، ينشيء الشخص أو المهاجم الضار مواقعًا ويحضرها إليك كما لو أنها من مصدر شرعي.

لذلك، من وجهة نظر المستخدم، يمكنك تعيين المعنى على أساس المحتوى الذي تراه عدة مرات، وبالتالي، فإن ذلك يكسب ثقة المستخدم ومن ثم تقدم المعلومات الخاصة بك. لذا، فبالنسبة لهذه الأنواع الثلاثة من الهجوم، إننا نرى أنواعًا مختلفة وضمن قارات مختلفة، قد يكون الانتشار - قد يكون التركيز مختلفًا.

فعلى سبيل المثال، في قارة آسيا، لا يكون الهجوم الهندسي الاجتماعي معنيًا بإنشاء صفحات الويب، لكن في الغالب ما يدعوك على الهواتف المحمولة أو إيقافك في جنبات الشارع. ويختلف هذا المستوى من الهجمات من قارة إلى أخرى.

ومع الاعتذار الشديد، إنني لا أعرف الكثير عن أي من هذه الأنواع تكون السائدة في أفريقيا، ولكن أريد أن أحدد السياق لك للتفكير في مشكلة في هذا المجال في الوقت الذي نمضي فيه في الاتجاهات الأمنية التي تؤثر على المسجلين.

الشريحة التالية من فضلك. الشريحة التالية. نعم التالية.

لذلك، عندما نتحدث عن نوع من التهديدات للمسجلين، هؤلاء المسجلون، هم الذين يسجّلون أسماء النطاقات أو أنك لديك اسم نطاق واحد في محفظتك أو قد يكون لديك العديد من أسماء النطاقات. ومرة أخرى، هناك نوعان من الهجمات. وإنكم لديكم هجوم خارجي وثمة هجوم داخلي أيضًا.

ومن المنظور الخارجي، فإنك تفترض وجود مهاجم نشط. وما سوف يفعله المهاجم عادة هو أنه، أو المؤسسة، تسعى للوصول إلى حساب تسجيلك والتحكم في جانب ذلك هو التحكم في اسم النطاق الخاص بك. أليس هذا صحيحًا؟ لذا، عادة ما يكون لك علاقة مع المسجل الذي يبيع الاسم لك أو مع البائع الذي تذهب إليه للحصول على النطاقات

الخاصة بك. وعادة ما يقوموا بالهجوم على حساب التسجيل. أما الهدف فيتمثل في التحكم في اسم النطاق الخاص بك.

وأما الجزء الآخر، ذي الصلة نوعًا ما، فهو أنهم يحاولون الوصول إلى حساب تسجيلك وهدفهم هو تغيير معلومات نظام اسم النطاق المرتبط باسم النطاق الخاص بك. ما الذي أعنيه بذلك؟ يمكنك تسجيل اسم نطاق، ومن المحتمل أن يكون لديك وجود على شبكة الإنترنت، ولديك موقعًا على شبكة الإنترنت أيضًا، ويمكنك تشغيل خادم البريد الخاص بك، وأن تمتلك هذه السجلات في حساب التسجيل.

عندما يتيسر للمهاجم الوصول إليه، سيُدخل هذا المهاجم مجموعة من السجلات الجديدة فضلاً عن تغييره لعنوان بروتوكول الإنترنت، حيث يتعين على الموقع الإلكتروني الانتقال إليه ورسائل البريد الإلكتروني أيضاً، وسيقوم بعمل ذلك بعدة طرق. وقد يرغب أيضًا في استخدام حسابك ونظامك كجزء من شبكة هجوم واسعة. أو أنه قد يرغب في استخدام هذا لتخريب صفحة الويب الخاصة بك ومحاولة الحصول على الأموال منها. وهذا ما أسميه التهديدات الخارجية.

وفيما يتعلق بالتهديدات الداخلية، فإنها تكون أسماء النطاق التي تمتلك سمعة وقيمة متبقية. فعند تسجيل أسماء النطاقات، فإن هذه الأسماء ستسجل معدلات التجديد التي تكون مرتفعة نسبيًا. وهذا لأن لديهم القيمة المتبقية، والسمعة، وهناك أيضًا، في بعض الحالات، تكلفة تحويل عالية جداً لتغيير اسم نطاق مختلف.

ونظرًا لامتلاك اسم النطاق الخاص بك قيمة، سيكون هناك أشخاص تراقب عن كثب اسمك. وإذا أخفقت في بعض الأحيان ونسيت تجديد اسمك وبعد فترة السماح، حسب اعتقادي، التي تبلغ خمسة أيام، سيقوم شخص آخر بتسجيل اسمك. وفي هذه الحالة، وفي ذلك السيناريو، يصبح الاسم ملكًا له. وإنك تتعرض لتكلفة عالية جداً وعملية مطولة للمطالبة باسترداد الاسم الخاص بك مرة أخرى. وبالتالي فإنني أرغب في تحديد السياق مع التفكير في هذا النوع من التهديد. وسأتولى استعراض ذلك بشيء من التفصيل.

حسنا، الشريحة التالية.

عندما نتحدث عن الوصول غير المصرح به إلى حساب التسجيل، فكيف يفعلون ذلك؟ كيف لك كمسجل أو كمهاجم القيام بذلك؟ وكما تعلمون، إنكم ترغبون في القدرة على فهم كيفية قيام المهاجم بذلك من أجل حماية أنفسكم.

أما النوع الأكثر وضوحًا فهو الهجوم التخميني. ففي هذا الهجوم يخمّن المهاجم اسم الحساب وكلمة المرور عند المسجل الخاص بكم. ولعلكم تتساءلون أنه من المحتمل أن يكون بعيد الاحتمال.

وقبل التحاقي بـ ICANN، كنت أقوم بأبحاث الدكتوراه التي تبحث في إمكانية استخدام أنظمة الأمن، وواحدة من الأشياء التي يقوم بها مختبرنا هي إلقاء نظرة على كلمات المرور، وكيفية تأمينها. وقد وجدنا أشياء مثيرة للاهتمام. تتجلى إحداهما في إعادة استخدام الأشخاص لكلمات المرور من خلال العديد من الحسابات المختلفة. ولديك تلك الكلمات المرورية لأعمالك البنكية ولحساب التسجيل الخاص بك، وإنك تمتلكهم وتعيد استخدامهم في العديد من الأماكن الأخرى، حيث يعني ذلك أنه عندما يحصل المهاجم على مجموعة واحدة من بيانات الاعتماد الخاصة بك، فإنه سيحاول استخدام ذلك لمجموعة أخرى من تسجيلات الدخول التي لديك، وهي إحدى نقاط الضعف.

أما نقطة الضعف الأخرى فهي ما نسميه فوضى كلمات المرور، التي تعني إمكانية التخمين ومدى صعوبته. إنها في غاية السهولة بالنسبة للتخمين. وبالتالي فإن المستشار الخاص بي صاغ ملصقًا من ألف كلمة مرور ومن غير المرجح أن يكون عشرات الآلاف من كلمات المرور وقد أجرى هذا التحليل والكلمات المرورية الشائعة، إنني أحبكم، وعادة ما تكون هي الأعلى من بينهم، وإنك لديك الكثير من الكلمات المرورية السهلة، ذات البساطة في التخمين. وبالنسبة للمهاجم فإن إحدى وسائله هي تخمين كلمة المرور الخاصة بك. ديف.

ديفيد بيستشيللو: كم منكم لديه كلمات مرور تكون أطول من سبعة حروف؟ حسناً. هل 10 أشخاص؟ عظيم جدًا. أم 15 شخصًا؟ حسنًا. في ICANN، طلب منا الحصول على كلمات

مرور من 20 حرفاً أو أكثر، التي يمكن أن تكون صعبة جداً. كم منكم يستخدم بعض أنواع من مدير كلمات المرور بشأن جهاز الكمبيوتر الخاص بكم حيث إنكم تحتفظون بكلمات المرور الخاصة بكم مشفرة؟ وهي واحدة من الأشياء التي يتعين عليكم أخذها بعين الاعتبار. حسنًا، فأنتم المناصرون هنا. لذا يتعين عليكم حقًا الأخذ بعين الاعتبار استخدام مدير كلمة المرور. وينشيء عديدًا من كلمات المرور القوية لك ويحافظ عليها بشكل آمن مخزنة على جهاز الكمبيوتر الخاص بكم مع التشفير، ويمتلك العديد منها برامج Android أو iPhone أو iPads حتى أنه يمكنكم استخدامه على جميع الأجهزة الخاصة بكم، وذلك أمر بالغ الفائدة للقيام به.

وأريد أيضًا أن أشير إلى أن تخمين كلمات المرور هي في الواقع ليست الطريق الأسهل للمهاجمين. أما أسهل طريق للمهاجمين في هذه الأيام هو خرق قاعدة بيانات كلمات المرور في موقع إلكتروني قمت بزيارته، ثم إجراء افتراضات، كما قال ستيف، التي تتمثل فيما إذا قمت بإنشاء كلمة المرور هذه، وكنت قد استخدمتها في أماكن أخرى، وحتى إذا ما كان ما يمكنهم القيام به هو الذهاب إلى الآلاف من المواقع التي تستخدم البرمجة النصية وعنوان البريد الإلكتروني الخاص بك، وسوف يجربون عنوان البريد الإلكتروني الخاص بك وكلمة المرور في آلاف المواقع، آملين في اختراق أحد المواقع التي قمت بزيارتها، حتى يمكنهم الحصول على تلك المعلومات.

وهذا السبب الذي يكمن وراء أهمية عدم استخدامكم نفس كلمة المرور للخدمات البنكية الخاصة بكم أو مثلما تفعل بأي شيء آخر. والأهم من ذلك، إذا كنت تستخدم الخدمات البنكية في بنوك متعددة، فاستخدم دائماً كلمة مرور مختلفة لكل من هذه البنوك.

ستيف تشينغ: شكرًا لك، ديف. وللمضي بسرعة، هناك طرق أخرى يمكن للمهاجم الحصول عليها من المضيف الذي يحتوي على بيانات الاعتماد. وقد يكون ذلك جهاز الكمبيوتر الخاص بك أو الخادم. وفي بعض الأحيان نقوم بتخزين بيانات الاعتماد هذه في نص واضح. وتحتفظ زوجتي أحياناً بملف Word، مع إدراج جميع كلمات المرور، وجميع حسابات

تسجيل الدخول التي لدينا. ويعد ذلك صحيحًا، أعني، حتى بالنسبة للمتخصصين في مجال الأمن، ومن ثم نتحرك نحو، كما ذكر ديف، مديري كلمات المرور.

وهناك طريقة أخرى، تتحدث عن الهندسة الاجتماعية، ونحن نتحدث عن هجمات التصيد والتصيد بالرمح. وعادة ما يكون التصيد والتصيد بالرمح الخطوة الأولى للاختراق للدخول إلى جهاز الكمبيوتر. وما يريدونه عادة هو تثبيت جزء من برامج، نسميها البرامج الضارة، التي يمكن أن تحصل على ما تكتبه ويمكن أن تتصدى له، وفي بعض الأحيان تتصدى لما تقوم بإرساله.

وهذا هو السيناريو النموذجي. قد تتلقوا رسالة بريد إلكتروني من المسجل الخاص بكم قائلة: "تنبيه، تنبيه! هناك نشاط غير مسموح به على حسابك". مع وجود أصوات. قد تفكر وتقول "حسنًا ولما لا". وتكون هناك العبارة التالية أيضًا "يرجى التسجيل هنا للتأكيد على عدم حدوث تغيير لأي شيء". وبالتالي فإن ذلك شائع تمامًا من وجهة نظر المسجل والتسجيل في بعض الأحيان. ومن الواضح أنه لم يتم إرسالها من مسجل. وعندما تقوم بالتسجيل، سيتم اختراق حسابك أو في بعض الأحيان يطلبون تنزيل شيء ما لمساعدتك في عملية التأمين. وفي هذه الحالة، سيثبت الجهاز الكمبيوتر الخاص بك برنامجًا ضارًا حيث تتعرض المعلومات الإضافية، وليس حساب التسجيل فقط، للخطر.

الشريحة التالية.

يعد الدخول غير المسموح به هو الخطوة الأولى. وهو وسيلة لتحقيق غاية. وليس غاية في حد ذاتها. إذا، ما هي الغاية هنا؟ الغاية هي تغيير معلومات تكوين نظام اسم النطاق الخاص بكم.

وإنه يقوم بذلك بطريقتين. فإنهم يغيرون خادم الاسم الخاص بكم لشيء آخر، خلاف العنوان المقصود. وبطبيعة الحال، ما يحدث سوف يؤدي إلى خسارة أو انقطاع من الخوادم الخاصة بكم، إذا كان هو الموقع الإلكتروني الخاص بكم أو البريد الإلكتروني الخاص بكم، وأنه يتم إعادة توجيه حركة المرور إلى خادم الهجوم. ويمكن أن يدخل أحيانًا انعدام التنسيق أو الخطأ الإداري أيضًا تغييرات بنتائج مماثلة.

الشريحة التالية.

هناك جانب آخر حيث يكون الوصول المسموح به نذيرًا... وهم يرغبون في تغيير المهاجم لمعلومات الاتصال على حسابكم. فما السبب وراء رغبتهم في القيام بذلك؟ إنهم يرغبون في القيام بذلك للسيطرة على اسم النطاق الخاص بكم. وفي هذه الحالة، يتم نقل أو السيطرة على نحو غير شرعي على اسم النطاق. وهذا ما نسميه اختراق النطاق. ومن الواضح أن الشيء الآخر الذين يقومون به هو أنهم يريدون عرقلة توصيل الخادم لمراسلات المسجل. وعادة ما يكون الشيء الأول الذي يقوم به المهاجمون هو تسجيل الدخول إلى النظام، وهم يغيرون من عنوان البريد الإلكتروني حيث يتصل المسجلون بكم.

بالتالي، إذا كنت تعتمد على قناة اتصال مع المسجلين للحصول على معلومات هامة، فإنك لن تستلمهم الآن. ولكن في العديد من الحالات، يتلقى العديد منا الكثير من رسائل البريد الإلكتروني يوميًا، بالتالي إذا كنت لا تتلقى أي منها من المسجل، يمكنك تجاهلها حتى في بعض الأحيان تكون متأخرة جدًا. وكانت هذه هي وجهة نظري.

ونظرًا لإدخالهم معلومات خاطئة، فيمكن أن يؤدي ذلك أيضًا إلى رفع تقرير عن عدم دقة نظام WHOIS ضدك، الذي يمكن أن يفضي إلى حدوث تعليق أو حذف لاسم النطاق من جانب المسجل. ومع وجود أمين سجل جديد في موضعه، هناك مستوى معين من التحقق من الدقة ويمكن أن يؤدي الإخفاق في دقة نظام WHOIS إلى التعليق.

وأخيراً، فإنه سيؤدي فقط إلى حذف تسجيل اسم النطاق من قبل الطرف غير المسموح به. بالتالي، يعد ذلك نوعًا من النظرة العامة عالية المستوى للتهديد كمسجل الذي قد تواجهه وكيفية قيام المهاجمين بذلك. وقبل الخوض في أي أمور أخرى، أود أن أفتح الأمر إلى حد طرح الأسئلة.

غابرييل بومبابو بوسيكو: نعم. أود أن أعرف إذا كانت ICANN - اسمي هو غابرييل. وأنا من الكونغو، من العاصمة كينشاسا وأود أن أعرف هل تتخذ ICANN خطوات للعمل مع الحكومات التي تكون مسؤولة عن التهديدات والهجمات الخارجية ضد المستخدمين النهائيين؟ ولدينا العديد من أعضاء المعارضة السياسية، وقد شهدنا استخدام تلك الهجمات الواردة من الحكومة ضد المواقع السياسية المعارضة. هل تفعل ICANN شيئًا حيال ذلك؟

ستيف تشينغ: اسمح لي أن أرى ما إذا كنت أفهم سؤالك بشكل صحيحي أم لا. إنك تتحدث عن حالة تقوم فيها الحكومة بمهاجمة مستخدم في بلده أو مهاجمة مستخدم في بعض البلاد الأخرى. لذا فهناك شيئان مختلفان. أحدهما هو التعسف والآخر هو الإرهاب.

وليس لدينا دور في هذا النوع من التداخل. فدورنا، حتى في مجال الأمن، هو التيسير والخبرات الموضوعية في المقام الأول.

إذا عملنا مع أي حكومة، عادة ما يكون هناك شيئًا يرتبط بالرقابة السيادية على نطاق المستوى الأعلى لرمز البلد. لذلك، على سبيل المثال، لدى ICANN علاقات مع 261 نطاق من نطاقات المستوى الأعلى لرمز البلد حيث تكون المعلومات الخاصة بهم في نظام أسماء النطاقات ويمكن للأشخاص الانتقال إلى أسماء النطاقات أو المواقع الإلكترونية أو تلقي رسائل البريد من المواطنين والمستخدمين في أي دولة، وسيتم توجيههم جميعًا بشكل صحيح من خلال عملية تحليل الاسم.

وهذا هو دورنا الأساسي عن طريق ما نسميه هيئة الإنترنت للأرقام المخصصة، التي تكون الآن حسب اعتقادي المعرفات التقنية العامة، وهي هيئة الإنترنت للأرقام المخصصة لما بعد المرحلة الانتقالية. أليس هذا صحيحًا؟ وسوف نعمل عادة، على المستوى التشغيلي لفريقي، في التهديدات لنظام اسم النطاق العالمي. لذا، قد نعمل بالتعاون مع الحكومات إذا ما تعرض موقع حكومي لهجوم عن طريق هجوم حجب الخدمة.

وقد تتذكرون منذ سنوات أن الموقع الإلكتروني لحكومة جورجيا قد تعرض لهجوم وبالتالي عملنا مع أشخاص من الأمن التشغيلي لمحاولة صد الهجوم. ولكن لم يتم إشراكنا في أي نوع من أنواع المواجهة أو الصراع بين أي طرف، الحكومة /الحكومة، أو المستخدم/المستخدم، أو الحكومة/المستخدم.

شخص غير محدد: لدي سؤالين، وملاحظة واستفسار. هناك ما نسميه [غير مسموع]. فعندما تقومون بكتابة اسم نطاق، فإنكم ستقعون في خطأ إذا كان لديكم سطوًا إلكترونيًا ناجمًا عن الخطأ المطبعي لإعطاء الانطباع للمستخدم بأنكم في وضع معين وأنكم غير ذلك. فالسطو الإلكتروني الناجم عن الخطأ المطبعي يشبه صفحة ويب من أحد البنوك، ولا يكون مثلها.

وسوف يكون سؤالي الثاني على بعد ما ذكره غابرييل. فقد تحدث غابرييل عن الحكومات والمواطنين وإننا نرغب في معرفة إذا كانت المخاطر والتهديدات التي نواجهها مع الانتخابات، لا سيما عندما يكون لدينا ولايات عديدة مثل ذلك محتملة الحدوث في الولايات المتحدة.

ديفيد بيستشيللو: أجب عن السؤال الأول. أعتقد أنكم تتحدث عن السطو الإلكتروني. هناك بعض الإرشادات وبعض القواعد بخصوص السطو الإلكتروني في سياسة ICANN التي يمكنك التقدم بطلب للحصول على هذا الاسم المحذوف من نظام اسم النطاق. وهناك بعض التهديدات التي تتطور فعلاً من السطو الإلكتروني الناجم عن الخطأ المطبعي فيما يسمى بإعادة كتابة تحليل الاسم، وهذا شيء يستخدم في الواقع من قبل الكيانات التجارية. وما يحدث معني بفندق أو مقهى، أو أي شخص يقدم الاتصال اللاسلكي، سوف يشترك مع شخص يرغب في طبع أخطاءك الكتابية، وحتى إذا قمت بكتابة www.ebay.com، فهذه الخدمة التي يشترك فيها الفندق أو الكشك سوف تأخذ

الإجابة من الإنترنت التي تذكر أنه لا يوجد مثل هذا الاسم وستوجهك إلى صفحة بحث تروج لها شركة، حسب اعتقادي، واحدة من الشركات تسمى [بير فروتس].

وتكون الصفحة بها إعلانات ولم تكن الصفحة التي ترغب في الذهاب إليها. أما ما ترغب حقًا في معرفته هو، لقد كتبت بالخطأ وإنني لم أصل إلى موقع eBay كما توقعت. وهذا في الواقع يشكل تهديدًا وكتبت اللجنة الاستشارية للأمن والاستقرار تقريرًا عن هذا منذ بضع سنوات وقمت بكتابة مدونة لمتابعة ذلك. وهذا سيء للغاية لأن ما يفعله هو أنه يخبرك بالأكاذيب. ويخبرك أن هناك مكاناً لقصده له هذا الاسم حيث لا ينبغي أن يكون هناك، وينبغي أن تكون الإجابة لا.

وذلك شيء عليك أن تكون على دراية به وأنت تعمل في مكان ما عن بعد، وواحد من الأشياء التي أود أن اقترحها عليكم هي أن تقوموا بتكوين جهاز كمبيوتر محمول أو هاتف خاص بكم دائماً لاستخدام خادم اسم تثقون به، سواء كان ذلك خادم OpenDNS أو Google أو خدمات الأسماء الكبيرة الأخرى. وبالنسبة لخادم Google فيسهل تذكره للغاية. إنه يكون 8.8.8.8، بالتالي فإنني أخبر الأشخاص بأنه إذا كنتم على دراية بكيفية فتح تكوينكم ويمكنكم الانتقال ووضع ذلك بشكل ثابت، فلن تكون هناك أهمية لمكان مضيكم، وستحصلون دائمًا على نفس تحليل الاسم ولن تجدوا أي أكاذيب. وهذا ما أود اقتراحه للتصدي للسطو الإلكتروني.

ستيف تشينغ: دعوني أحاول الإجابة على السؤال الثاني، حيث هذا النوع من التصيّد والاحتيال أو الهجمات الأمنية التي تُعرض بيانات دخول المستخدم النهائي للخطر، مما يؤدي إلى سرقة رسائل البريد الإلكتروني الذي يحدث على أعلى مستوى. وأظن أنه لا ضير من القول بأن هذا الأمر خارج اختصاص ICANN، لأن اختصاص ICANN يتمثل في تنسيق تخصيص المعرفات وتفويضها.

ومع ذلك، أظن أنه حتى موظفو منظمتنا يحتاجون إلى خوض هذه التدريبات حتى لا نقع، كموظفين، ضحايا لهذه الهجمات الاحتيالية، ولقد أجريت بحثًا في هذا الصدد على

المستوى الشخصي، وبالتالي يُمكنني الحديث في هذا الأمر وتزويدكم ببعض المؤشرات فيما بعد، ولكنني أؤكد أن هذا الأمر حقًا لا يخص ICANN. فليس من مهام ICANN أو اختصاصها أن تُثقف المستخدمين بخصوص هذا النوع من الهجمات.

ديفيد بيستشيللو: في الواقع، لا يندرج هذا الأمر ضمن اختصاصنا، ولكن من ضمن الأشياء التي يفعلها فريقي، نشر مقالاتٍ دورية حول المصطلحات والتهديدات الأمنية؛ فعلى سبيل المثال، أقوم اليوم بنشر مقالاً حول محتوى الويب غير المتاح في نشرة ICANN الإخبارية. وقد نشرنا مقالاتٍ حول هجمات التصنت عبر الإنترنت والقنوات السرية وأشياء أخرى، فإذا ذهبتم إلى مدونة ICANN وبحثتم عن مصطلح أمن، فغالبًا ستجدون شيئًا مما نشرناه من الأمور المفيدة على مستوى مستخدمي الإنترنت. والمحتوى متوسط من الناحية التقنية، إلا أن الفكرة فيه هي مساعدة الناس على فهم التهديدات المختلفة.

عزيز هلالي: شكرًا جزيلاً. ما زال لدينا أربع أشخاص يطلبون الكلمة، لذا أرجو محاولة الإسراع. تيجاني أولاً ثم [غير مسموع]. تيجاني، الكلمة لك.

تيجاني بن جمعة: أظن أن ستيفن أجاب عن الأمر، ولكنك عندما أجبت على سؤال غابرييل، أظن أنك لم تذكر أن الأمر خارج اختصاص ICANN لأنها مسؤولة عن المعرّف الفريد. فأمن خوادم الجذر هو مهمة ICANN، ولكن أي شيء بين المستخدم والحكومة وأمين السجل هو عقد بين المستخدم وأمين السجل. وبالتالي، لا يُمكن أن تتدخل فيه ICANN ولا علاقة لها به. شكرًا.

ديفيد بيستشيللو: أود فقط أن أصحح لك شيئًا بخصوص أمن خوادم الجذر. في الواقع لا تتحمل ICANN مسؤولية أمن خوادم الجذر. فمسؤوليتنا تنحصر في شفافية منطقة الجذر،

وبالتالي فإن كل مشغل لخادم الجذر مسؤولٌ عن التشغيل الخاص به. فمسؤولية ملف الجذر L تقع على عاتق ICANN، ونحن نأخذ الامر بجدية تامة، وأظن أننا نقوم بعملٍ رائع. ولكن مجتمع الإنترنت في الصين (ISC) ووزارة الدفاع الأمريكية والشبكات الأوروبية لبروتوكول الإنترنت وآخرون، هم المسؤولون عن تشغيل خوادم الجذر الخاصة بهم.

عزيز هلالي: شكراً لك ديفيد. [غير مسموع]، إليك الكلمة.

شخص غير محدد: شكرًا. [غير مسموع]، اتحاد المستهلكين من [غير مسموع]. بصفتي ممثلاً عن المستهلكين، أود أن أسأل ICANN عما إذا كان لديهم بياناتٍ إحصائية لمعرفة نوع الخطر في كل منطقة. فعلى سبيل المثال، إذا أردتُ اليوم تنظيم حملة أمنية حتى نتمكن من قول، "حسنًا أفريقيا، ليس لديكم مخاطر، ولكن هل لدينا بيانات إحصائية لمعرفة ماهية الخطر في كل منطقة حتى نتمكن من قول أنكم لستم بلدً ا غنية جدًا ولكن يجب عليكم الحذر من هذا النوع من الخطر الموجود في هذه المنطقة". شكرًا.

ستيف شينغ: إذا كان فهمي صحيحًا من وجهة نظر ICANN، فالسؤال هو، هل نمتلك بيانات تهديدات لكل منطقة. لستُ متأكدًا من ذلك، لأنني لا أعرف كيف نحصل على تلك البيانات في بعض الحالات. أليس هذا صحيحًا؟ إن اختصاصنا ضيق وتمتد بياناتنا إلى الحد الممكن، وقد تمتلك معظم شركت الأمن بعضًا من هذه البيانات. وقد يمتلكها بعض أمناء السجل، ولكن الأمر ليس واضح بالنسبة لي، ولسوف أنظر في هذا الأمر، ولكنني أُقر أن هذا سؤالٌ في محله. فدعني أنظر في هذا الأمر وأعود إليك.

ديفيد بيستشيللو: ربما لا تمتلك ICANN بينات التهديدات على المستوى الإقليمي. إلا أنك إذا ذهبت إلى مجموعة عمل مكافحة التصيّد، فستجد لديهم تقريرًا عن الحركية ومخاطرها، وربما يكون عمر هذا التقرير عامان الآن، وقد كان نظام التشغيل النقَّال واحدًا من ضمن المخاطر الكبيرة في منطقة أفريقيا، حيث تجد، مثلاً، عددًا كبيرًا من مزودي الخدمة في أفريقيا لا يُقدمون تحديثاتٍ تلقائية لأنظمة أندرويد، والعديد من الأجهزة المُباعة في أفريقيا غير قابلة للتحديث بعد عددٍ معين من تحديثات نظام التشغيل، وذلك بسبب الحاجة إلى الحفاظ على انخفاض السعر. وبالتالي أصبح هذا الأمر يُمثل مشكلة بسبب استمرار نقطة الضعف هذه بين جميع مشتركي هذا المزود لمدةٍ طويلة جدًا. وبالتالي من ضمن الأشياء التي يمكن لكل بلد النظر فيها للحد من التهديد لمستخدميها، التفكير ووضع معايير أو التزامات للمزود للحفاظ على ما نسميه عملة التصحيح على أنظمة التشغيل، وهو ما يُعتبر تحديًا لأنها مسألة اقتصادية.

فإذا أردت جلب جهاز لملايين من الناس بسعرٍ منخفض جدًا، فإن ما ستفعله في الغالب هو توفيق حجم الذاكرة التي ستضعها في الجهاز، ومن ثم تضع نظام تشغيل أكبر لإضافة المميزات، وبالتالي لا يمكنك وضع كل شيء في هذا الجهاز الصغير. وستجد لسان حال المزود يقول، "حسنًا، كيف يمكنني خدمة الناس بجهازٍ رخيص وأحافظ على أمن الأجهزة؟" وبالتالي فهذا تحدٍ أظن أنه يواجه هذه المنطقة، بسبب وجود عددًا من الدول الناشئة من الناحية التقنية.

وأنا أحاول التفكير. وأعرف أن شركة سيمانتك لديها إحصائيات إقليمية على موقعها، وأن شركة ماكافي لديها على موقعها بعض الإحصائيات الإقليمية الخاصة بالتهديدات. وتوجد حاليًا الكثير من الشركات التي تحاول الترويج لبرامج أمن ضد برمجيات الدفع القسري للفدية. هل يعرف الجميع ما هو هجوم برمجيات الدفع القسري للفدية؟ من الذي لا يعرف هجوم برمجيات الدفع القسري للفدية؟

حسنًا، عادةً ما يكون هجوم برمجيات الدفع القسري للفدية عبارة عن هجوم عن طريق البريد الإلكتروني، وعندما تستلم مستندًا أو بعض المرفقات على البريد الإلكتروني، وعند الضغط عليه، يتم تثبيت برنامج على جهاز الكمبيوتر الخاص بك، ومن ثم

يتواصل هذا البرنامج مع كمبيوتر آخر ويقوم بتنزيل برنامج تشفير ويُشفِّر جميع البيانات على جهاز الكمبيوتر الخاص بك ثم يقفل شاشتك أو يقفل الجهاز، وأحيانًا يُحاكي الشرطة أو أحد الهيئات الضريبية، ويقول، "لقد تم خطف جهاز الكمبيوتر الخاص بك. ويجب أن تدفع غرامة مالية لهذا العنوان أو هذه الجهة، وإلا سنمحو بياناتك للأبد". وما يفعله المهاجم هو خطف جهازك مقابل فدية، وإذا دفعتها، فمن المفترض أن تحصل على المفتاح الذي يُمكنك من فك تشفير بياناتك.

وإذا كنتم مهتمون بمعرفة المزيد عن هذا الأمر، لأن الوقت ليس ملكنا، فقد كتبت بعض المقالات بخصوص هذا الأمر على مدونة ICANN وقدمت أيضًا بعض العروض التقديمية سيشاركها معكم العاملين في اللجنة الاستشارية العامة لعموم المستخدمين ويوزعونها عليكم. وهذا نوع آخر من الهجمات الكبيرة جدا، والعالمية أيضًا، ولكنهم يبذلون مجهودًا عظيمًا في ترجمته إلى لغاتٍ محلية. فحتى الشاشات التي تعرض باللغة العربية أو الفرنسية، واللغات المحدودة جدًا، إنها في غاية التطور.

عزيز هلالي: شكرًا جزيلاً. لا يزال لدينا الكثير من الأسئلة، ولدينا أسئلة عبر الدردشة، وبالتالي سنحاول الإسراع أكثر.

[سيرج]: مرحبًا بالجميع. معكم [سيرج] من الكونغو برازافيل. لديَّ سؤالين سوف أطرحهما. يدور السؤال الأول حول تأثير بروتوكول الإنترنت- الإصدار السادس، من جهة تأثير بروتوكول الإنترنت- الإصدار السادس على نظام اسم النطاق. فهل يتعلق ذلك بفشلٍ ما؟ وإذا كان هناك فشل، فكيف يمكننا حل هذه المشكلة؛ أما سؤالي الثاني هو، ما هي إمكانية تطبيق نظام لمراقبة مسائل الأمن في الدول؟ وهل ستساعدنا ICANN في هذا الأمر. شكرًا.

ستيف شينغ: حسنًا، بالنسبة لسؤالك عن إنشاء مراكز مراقبة، فأظن أنه من العادل القول بأن الأمر بعيد عن اختصاص ICANN. ومن ضمن الموارد التي قد تكون متوفرة لكم، ما نسميه (CERT)، وهو فريق الاستجابة لحالات طوارئ الحاسب الآلي الذي يوجد في العديد من الدول وفي الولايات المتحدة، كما يوجد أيضًا مركز تنسيق فريق الاستجابة لحالات طوارئ الحاسب الآلي. فإذا كنتم تفكرون في هذا الطريق، فإنني أرشح لكم التواصل معهم والحصول على بعض المساعدة من هناك.

ديفيد بيستشيللو: يجب أن تعرفوا أن ICANN لا تحكم الإنترنت. بل هي أقرب ما تكون إلى مجرد مدير وتتمثل مسؤوليتها في تفويض المعرِّفات. ومن ضمن الأمور التي نقوم بها، تسليم مسؤولية أسماء النطاق إلى سجلات نطاق المستوى الأعلى، ويتولون هم مسؤولية ما نفوضه لهم. وبالتالي فإن شركة فيري ساين هي المسؤولة عن .com. فلا يمكننا أن نذهب إلى فيري ساين ونقول لهم "افعلوا هذا"، إلا إذا انتهكوا تعاقدنا معهم. لا يمكننا أن نقول لهم "أزيلوا اسم نطاق". ربما تتمكن جهة إنفاذ قانون أو أحد الأشخاص من القيام بذلك مع فيري ساين بشكلٍ مباشر.

ومن ضمن الأمور التي تأتي في إطار تحديد السياق الخاص بإجابتي التالية، أنواع التهديدات التي نرصدها في ICANN عبر عملياتنا المركزية، ألا وهي نظام الاسم في المستوى الأعلى وفي الجذر. ولدينا برنامج في عملياتنا في ICANN نقوم من خلاله بالتحقق للتأكد من عمل ما نسميه اسم الخوادم الرسمية وتجاوبه، وعندما نكتشف أنه غير فعال، نتصل بهم؛ وبالتالي فنحن لدينا عملية تشغيلية في أعلى مستوى من أسماء النطاقات، نحاول من خلالها ضمان توافر مساحة اسم الخادم ومرونته وسلامته من الأخطاء، وقد يكون ذلك أقصى تدخل تشغيلي نقوم به.

كما أننا نجري اختبارات للتأكد من تعيين جميع ملفات المنطقة الموجودة في المستوى الأعلى الذي يدعم الامتدادات الأمنية لنظام اسم النطاق، والتأكد من عمل التوقيعات بشكلٍ صحيح، وبالتالي نقوم أيضًا بمراقبة شفافية تشفير المستوى الأعلى.

عزيز هلالي: شكراً لك ديفيد. أود منح الكلمة لمن يريدون طرح الأسئلة، لذا أرجوا ألا يستغرق السؤال أكثر من دقيقة ودقيقتين للإجابة. لديَّ الآن، بكاري علي [غير مسموع]، وبعدها سنرى إذا ما كان لدينا وقت للأسئلة على الدردشة. بكاري، إليك الكلمة.

بكاري: شكرًا جزيلاً. محدثكم بكاري، عضو جمعية الإنترنت من مالي. ولدي سؤال حول المستخدمين النهائيين. نعرف أن بعض الهيئات تكون هي الهدف من هذه الهجمات، ولكن المستخدم هو من يدفع الثمن الأكبر، فهل توجد هجمات منها توجه خصيصًا إلى الهيئات أو المستخدمين النهائيين؟ هذا هو السؤال الأول.

أما السؤال الثاني، فيدور حول اسم النطاق. فالمستخدم النهائي ليس هو المسؤول. فإذا ظننت أن النطاق الخاص بي قد تمت مهاجمته، فهل يمكنني أن أطلب من السجل حل مشكلتي؟

عزيز هلالي: حسنًا، سنتلقى ثلاثة أسئلة ثم نُجيبك. علي، إليك الكلمة.

علي المشعل: الأسئلة. مجرد توضيح أطلبه من ستيف حول عرضه التقديمي، تجديد النطاق؛ هل قلت أن لديك خمسة أيام أم 30 يومًا؟ وما السبب، ومن الذي حدد هذا؟ وهل هذا من عمل أمناء السجل أم من السجل نفسه؟ يبدو أن هناك بعض الانحراف لأن المدة عادة ما تكون، على حد علمي، حوالي 30 يوما، ولكني الآن أسمع أنها خمسة أيام، فأين الانحراف إذًا؟ هذا هو الأمر الأول.

أما سؤالي الثاني، عفوًا لم أتمكن من معرفة اسمه، السيد المحترم الذي يجلس بجوار ستيف ويرتدي قميصًا أصفر. هذا هو أنتم. ديفيد. ديفيد، لقد تحدثت عن مديرين كلمة

المرور. ولقد تجنبتُ طواعيةً الاستعانة بمديرين كلمة المرور، لأنني ببساطة أشك بأنك تضع البيض كله في سلةٍ واحدة. فإذا ما قام شخصٌ ما بقرصنة الكمبيوتر الخاص بك، فإنك بذلك تكون قد قدمت له جميع كلمات مرورك على طبقٍ من فضة. فأرجو أن تُصحح لي هذا الافتراض أو تؤكده. شكرًا.

شخص غير محدد: حسنًا، سؤال واحد فقط. لدي سؤالان. محدثكم [غير مسموع] من جمهورية الكونغو. لدي سؤالان. أولاً، أود أن أعرف، هل تمتلك ICANN حلًا أو يمكنها فرض عقوبة على الهجمات الصادرة من دولة على دولةٍ أخرى؟ والسؤال الثاني، هل لديكم في ICANN نظامًا لدراسة التطبيقات الجديدة الموجودة على الإنترنت، بحيث يُمكنكم معرفة ما إذا كانت تشتمل على بعض الأضرار للمستخدم، ومحاربة الهجمات؟ شكرًا.

ستيف شينغ: خالص اعتذاري لكم. يجب أن أذهب قريبًا جدًا لدعم جلسة أخرى. ولكن بالنسبة لفترة سماح تجديد النطاق، أظن أن هناك فترات سماح متعددة. وربما تكون الفترة التي تتحدث عنها هي مجموع للفترات لتبلغ 30 يومًا. ويجب أن أعترف بأنني لست خبيرً في هذا المجال، ولكنني _ سأتعاون أنا وديفيد - وسنوافيك بالمعلومات الصحيحة.

أما بالنسبة لسؤال نظام WHOIS والسبب في أن المستخدم هو المسؤول، فأظن أننا جميعًا نتشارك المسؤولية في بعض الأحيان، أليس كذلك؟ وأقصد من وجهة نظر أوسع، أن المرء يرغب في إسناد المسؤولية للشخص الذي يُمكنه فعليًا حل المشكلة. وأظن أن المستخدمين يلعبون دورًا هامًا في ذلك. ولا يُمكننا الاعتماد في كل شيء على المشتركين والسجلات، بسبب سلوكياتنا الخاطئة. بل علينا دور في ذلك. ولا يخفى على أحد أن أمناء السجلات والسجلات يتحملون مسؤولية أنفسهم، أليس كذلك؟ وبالتالي، أظن أنه قتالٌ ضدنا جميعًا، وكلٌ منا له دور، ولكن يجب أن نُحمِّل المسؤولية للجهات والأشخاص الذين يمكنهم حل المشكلة.

وهاتان هما إجابتاي السريعتان. أعتذر. يجب أن أغادر، ولكن أعتقد أن زملائي من اللجنة الاستشارية العامة لعموم المستخدمين لديهم صلاحياتي، وعناوين بريدي الإلكتروني، وبالتالي ياسيم أو أيريل لديكم مُطلق الحرية في التفويضات ويُسعدني أن أجيب على هذه الأسئلة عبر البريد الإلكتروني. شكرًا.

ديفيد بيستشيللو: شكرًا لك، ستيف. سأتمكن من البقاء لفترةٍ أطول قليلاً، ويسعدني أن أحاول الإجابة على أكبر قدر يمكنني تذكره من هذه الأسئلة. فأنا أتقدم في السن وأهرم، وهذا تحدٍ بالنسبة لي. أردت التعليق أو متابعة ما قاله ستيف بخصوص المسؤولية والمساءلة.

عندما تُسجل اسم نطاق، فإن الامر يُشبه استئجار شقة أو منزل، أو الحصول على رخصة قيادة. فأنت الآن من يتحمل المسؤولية، وأنت من يُقرر ما سيتم فعله باسم النطاق هذا. ومن ضمن الأشياء التي يُمكنك فعلها باسم النطاق، تشغيل خادم بريد. ويُمكنك أيضًا استضافة موقعًا إلكترونيًا.

فمن الذي ستختاره ليشغل لك خادم البريد هذا؟ غالبًا ستختار مزوّد خدمة إنترنت، وقد تحصل أحيانًا على هذه الخدمة من طرف خارجي. وقد تستضيف مدونتك أحيانًا على Typepad. وربما تستضيف موقع ويب على مُشغل ويب محلي.

وبالتالي أصبح لك الآن شريكًا آخر، دفعت له أو اعتمدت عليه لتزويد استضافتك، فأنت إذًا مسؤول عن الاسم ولكنه مسؤول عن تشغيل موقع الويب. أليس هذا صحيحًا؟ ويختلف هذا الأمر في العديد من الحالات، ما بين أمين السجل الذي تحصل منه على الاسم وبين السجل الذي حصل منه الأمين على الاسم.

وبالتالي هناك أجزاء عديدة مختلفة من حيث الحركة، أو من حيث من يقوم فعليًا بوضع المعلومات أو نشرها أو إرسال بريد. فعندما يتعرض شخصٌ ما للهجوم، يكون من ضمن الأشياء التي تعنيني لكوني أعمل في الأمن التشغيلي، محاولة فهم مصدر الهجوم وما الذي تعرض للهجوم ومن هو الطرف المسؤول عن الهجوم ومن الذي يتحمل مسؤولية تصحيح التهديد أو تخفيفه، وهذا ليس بالأمر الهين. فالأمر في غاية التعقيد،

بل ويزداد تعقيدًا عندما يحدث على مستوى عابر لمناطق الاختصاص القضائي، كأن يكون خادم موقع الويب في هولندا ويكون الشخص المهاجم في كرواتيا ويقوم بإرسال بيت كوين لشخصٍ في أمريكا اللاتينية.

وبالتالي فقد وجدت وظيفتي غايةً في الإثارة، لأن المرء يواجه معضلة غاية في الصعوبة عندما يجمع بين العثور على مجرم ثم يُبلغ بإلقاء القبض عليه ووضعه في السجن. أليس هذا صحيحًا؟ وفي الواقع، لا تقوم ICANN بمثل هذه البلاغات، ولكن لا شك أننا نعمل مع جهات إنفاذ القانون لفعل مثل هذه الأمور. وأرجو أن أكون قد أجبت على سؤالك.

أيهما الرقم الصحيح، خمسة أيام، أم 30 يومًا؟ في الواقع، توجد فترات تعليق متعددة، وأولها تُسمى إضافة فترة سماح. ومنذ الوقت الذي تُكمل فيه التسجيل الفعلي لاسم النطاق، يكون أمامك خمسة أيام، تُسمى إضافة فترة السماح، لتؤكد على أن هذا هو الاسم الذي أردته. أجل. ففي بعض الأحيان يُخطئ الناس في الكتابة، حتى وهم ذاهبون للتسجيل، وبالتالي يكون لديك خمسة أيام يُمكنك أن تذهب خلالها وتقول "لا، لم يكن هذا هو الاسم الذي أردته"، ولا تُطبق عليك عقوبة ولا تخسر أموالك. فالأمر يُشبه إعادة رداء إلى المتجر. طالما تمتلك الإيصال.

وبعد ذلك، إذا سجلت اسم نطاق لمدة عام وانتهى العام ولم تقم بالتجديد الفعلي، فيكون أمامك 30 يومًا بعد انتهاء هذا العام يظل خلالها الاسم مُعلقًا ولا يمكن لشخصٍ آخر أن يسجله، بحيث يكون الاسم مُعلقًا فعليًا، وبعدها يكون أمامك 30 يومًا أخرى بعد انتهاء الصلاحية قبل أن يقول أمين السجل، "حسنًا، يبدو واضحًا أن هذا الشخص لا يريد الاسم. لذلك فسوف أعيد طرحه. هل ما ذكرته يجيب على أسئلتك يا علي؟

حسنًا. مدير كلمة المرور. تستخدم برامج إدارة كلمة المرور تشفيرًا قويًا. ولم أكن لأوصي لك أبدًا باستخدام مدير كلمة مرور لا يُشفِّر المعلومات، لأنه لا فائدة من فعل ذلك ووضعه في مفكرة. ولكن مُعظم برامج إدارة كلمة المرور هذه الأيام تستخدم تشفير AES 256-بت أو أقوى، وهو شيء لا يُترك هكذا لأي شخص كي يقرأه.

وتكمن قيمة مدير كلمة المرور في أنك يُمكنك تذكر كلمة مرور واحدة وإنشاء كلمة مرور قوية، وفي الواقع، الطريقة التي تعمل بها العديد من برامج إدارة كلمة المرور، هي استخدام كلمة مرور واحدة. ويمكنك ترك البرنامج ليولد لك جميع كلمات المرور ولن تضطر أبدًا إلى تذكرها، وسوف تُكتب تلقائيًا عندما تقم بزيارة موقع باستخدام كلمة مرور قمت بتوليدها. لذا، فإن ما أفعله في الغالب مع مدير كلمات المرور الخاص بي، أن أقول "اصنع كلمة مرور من 24 حرف". ولا أعرف ما هي كلمة المرور، ولكن في كل مرة أزور فيها ذلك الموقع، يقوم البرنامج بكتابته لي، وبالتالي لست مضطرًا للتذكر. وأعتقد أنه أمرٌ مفيد للغاية.

الهجمات من دولة إلى دولة. ICANN ليست جهة حكومية. ونحن لسنا شركاء في الأمم المتحدة. ولا نشارك في مجلس أوروبا إلا بصفتنا مراقبين. ولسنا شركاء في أي تفاعل بين الحكومات. ويتمثل تفاعلنا الوحيد مع الحكومات، في تعزيز الإنترنت المفتوح وتعزيز نظام اسم نطاق مفتوح وموحَّد، وتقديم الدعم للحكومات في عملياتهم الفنية الخاصة باسم الخدمة.

وبالتالي لسنا منظمة وضع سياسات في هذا الجانب. وليس لدينا أي سياساتٍ خاصة بعقوبات الحكومات فيما بينها. ماذا كان آخر سؤال؟ التطبيقات الجديدة والمميزات. لسنا أيضًا جهة تطوير برمجيات أو وكالة اختبارات. فعلى سبيل المثال، إذا أردت شراء تطبيق من متجر iTunes أو Android Play أو مهما كان، فلا دخل لنا بالأمر إلا فيما يخص تطبيق ما قد نقم بتطويره.

في بعض الأحيان، في حالة وجود شيء ما يبدو أنه يؤثر على نظام اسم النطاق، وكنا نعرف أو لدينا علم بوجود مشكلة في أحد التطبيقات، فقد نكتب نوع من أنواع النصائح ونضعها على موقعنا الإلكتروني، ولكن هذا لا يدخل ضمن نطاق أنشطتنا العادية.

هل أجبتُ على جميع الأسئلة؟ لا، ولا بأس بهذا. فأنا أحاول فقط الإجابة على... أنت من جلب لي كل هذه الأسئلة. ولا يُمكنك أن تُخبرهم بأنني لا أستطيع الإجابة عليها.

عزيز هلالي: شكرًا جزيلاً. هذه الأسئلة توضح أن القرار كان مهمًا للغاية، لذا، نشكرك يا ديفيد أنت وستيف على هذا العرض التقديمي.

وسأطلب من المشاركين متابعة هذه المناقشة عبر الإنترنت، إذا كانوا مهتمين. وأظن أن الجميع مهتمون، لذا يجب أن ننتهي الآن لأننا يجب أن نغادر هذه القاعة لوجود جلسة أخرى الآن، ونود أن نمنح بعض الوقت للمترجمين الذين أود تقديم الشكر لهم. تيجاني، هل تريد أن تتحدث؟

تيجاني بن جمعة: شكرًا جزيلاً. بالنسبة لبرنامج بناء الوعي الخاص باللجنة الاستشارية العامة لعموم المستخدمين، فقد رتبنا ندوة عبر الويب مع ستيف بخصوص هذا الموضوع. فقد ناقشنا أمورًا كثيرة اليوم. وأرى أن الكثيرون مهتمون بالأمر. فإذا أردتم منا ترتيب ندوة عبر الويب بخصوص هذا الموضوع، فما عليكم سوى إخبارنا. ونحن لدينا رغبة في عقد بعض الندوات عبر الويب فيما يهم الجميع، فما عليكم سوى أن تطلبوا ذلك. شكرًا.

عزيز هلالي: حسنًا. طلب مني تيجاني إنهاء هذه الجلسة، لذا أتوجه بخالص شكري لكم. شكرًا لك يا ديفيد، ستيف. نشكر المترجمين والعاملين، ونراكم لاحقًا.

[نهاية النص المدون]