مسودة مايو/أيار 2023

المشورة: الامتثال لالتزامات مكافحة انتهاك نظام أسماء النطاقات DNS الواردة في اتفاقية اعتماد أمين السجل واتفاقية السجل

توفر هذه المشورة إرشادات حول تفسير وأيضًا الامتثال للتعديلات [تاريخ] على اتفاقية اعتماد أمين السجل (RAA) واتفاقية السجل (RA) القاعدية لنطاقات المستوى الأعلى العامة (gTLD) فيما يخص التزامات الحد من انتهاك نظام أسماء النطاقات (DNS) (ويشار إليها فيما يلي هنا بلفظ تعديلات انتهاك نظام أسماء النطاقات).

وفيما لم يرد فيه تعديل على وجه الخصوص من خلال تعديلات انتهاك نظام أسماء النطاقات DNS، فإن جميع التزامات اتفاقية اعتماد أمناء السجلات واتفاقية السجل اللتان كانتا ساريتان قبل هذه التعديلات تظل سارية ومعمول بها.

تحمل جميع المصطلحات والألفاظ المكتوبة بخطوط عريضة وغير معرَّفة في هذه المشورة المعاني الموضحة إزاء كل منها في اتفاقية اعتماد أمناء السجلات واتفاقية السجل.

أمناء السجلات والسجلات الذين يستعينون بالممارسات المنصوص عليها في المشورة يستوفون على الأرجح الالتزامات الموضحة في تعديلات انتهاك نظام أسماء النطاقات DNS، إلا أن الالتزام بواحدة أو أكثر من هذه الممارسات لن يفضي تلقائيًا عن قرار بأن أمين السجل أو مشغل السجل قد امتثل للالتزامات المفروضة عليه. وقد جاءت الالتزامات المنصوص عليها أدناه لأغراض التوضيح فقط وليس الهدف منها تقييد الإجراءات الممكنة للحد من الانتهاكات. وفي جميع الأحوال، كلما أطلقت إدارة الامتثال التعاقدي في ICANN استقصاءً، يجب على أمناء السجلات ومشغلي السجلات تقديم ما يثبت الالتزام بالمتطلبات ذات الصلة في اتفاقية اعتماد أمناء السجلات واتفاقية السجل.

نبذة تعريفية

تتعاقد منظمة ICANN مع السجلات من أجل تشغيل نطاقات gTLD من خلال اتفاقية سجل. وتنص اتفاقية السجل على مسئوليات مشغل السجل، والتي تشتمل على الحفاظ على قاعدة بيانات رسمية لجميع أسماء النطاقات المسجلة في نطاق gTLD ونشر منطقة DNS لنطاق gTLD.

كما تبرم ICANN أيضًا اتفاقية لاعتماد أمناء السجلات مع كل أمين سجل، وهو ما يتيح لأمين السجل عرض خدمات تسجيل أسماء النطاقات في نطاقات gTLD. وتنص اتفاقية اعتماد أمناء السجلات على المسئوليات المنوطة بأمين السجل، مثل توثيق معلومات المسجل (أو صاحب الاسم المسجل) والاحتفاظ بسجلات دقيقة. إن أدوار والتزامات أمناء السجلات والسجلات واضحة ومتميزة وهي موضحة في الاتفاقيات المبرمة مع كل منهم، أي اتفاقية اعتماد أمناء السجلات واتفاقية السجل.

لهيئة ICANN صلاحية وسلطة إنفاذ القواعد ذات الصلة بخدمات تسجيل أسماء النطاقات وأسماء النطاقات على النحو الموضح في اتفاقية اعتماد أمناء السجلات وفي اتفاقية السجل. تركز هذه المشورة على أسماء النطاقات (أو الأسماء المسجلة) في نطاقات gTLD التي يتم استخدامها كوسائل أو آليات من أجل انتهاك نظام أسماء النطاقات DNS. إن المتطلبات الخاصة بتعديلات انتهاك نظام أسماء النطاقات DNS الواردة في اتفاقية اعتماد أمناء السجلات واتفاقية السجل تقوم على أساس الإجراءات التي يمكن لكل من أمناء السجلات ومشغلي السجلات على التوالي اتخاذها من أجل الحد من نطاق وحدة الضرر والانتهاك الحادث بسبب انتهاك نظام أسماء النطاقات DNS. كما تراعي هذه المتطلبات بأن أمناء

السجلات ومشغلي السجلات يمثل فقط حصة من منظومة أسماء النطاقات، والتي تتألف من العديد من الجهات الفاعلة[1]. واستنادًا إلى الظروف النوعية لأي حالة من حالات انتهاك نظام أسماء النطاقات DNS، فإن الجهة الأنسب في اكتشاف وتقييم وتوثيق ووقف نشاط الانتهاك قد تتفاوت، وفي بعض الأحيان قد تكون جهة غير أمين السجل أو مشغل السجل.

انتهاك نظام أسماء النطاقات DNS

ولأغراض اتفاقية اعتماد أمناء السجلات واتفاقية السجل وهذه المشورة، يقصد بلفظ *انتهاك نظام أسماء النطاقات DNS* البرامج الضارة وشبكات بوت نت والتصيُّد والاستدراج والبريد غير المرغوب (عند استخدام البريد غير المرغوب كآلية إرسال وتنفيذ لأي من الأنواع الأربعة الأخرى من انتهاك نظام أسماء النطاقات DNS) حيث إن هذه المصطلحات محددة في القسم 2.1 من تقرير اللجنة الاستشارية للأمن والاستقرار حول أسلوب قابل للتشغيل البيني في التعامل مع معالجة الانتهاكات في نظام أسماء النطاقات (SAC 115[2]):

البرمجيات الضارة عبارة عن برمجيات ضارة يتم تثبيتها و/أو تنفيذها على أحد الأجهزة بدون موافقة المستخدم، وهو ما يؤدي إلى قطع وتعطيل عمليات الجهاز، كما تقوم بجمع معلومات حساسة، و/أو تحصل على الوصول إلى أنظمة كمبيوتر خاصة. وتشمل البرمجيات الضارة كلاً من الفيروسات وبرامج التجسس وبرامج الفدية وغيرها من البرمجيات غير المرغوبة.

شبكات بوت نت عبارة عن مجموعات من أجهزة الكمبيوتر المتصلة بالإنترنت تمت إصابتها ببرمجيات ضارة ومن الممكن توجيهها لأداء أنشطة تحت سيطرة مهاجم بعيد.

التصيُّد ويحدث عندما يقوم مهاجم بخداع أحد الضحايا من أجل الكشف عن معلومات شخصية حساسة أو تخص العمل أو معلومات مالية (على سبيل المثال أرقام حسابات أو بيانات تسجيل الدخول أو كلمات مرور)، سواء عن طريق إرسال رسائل إلكترونية احتيالية أو متشابهة، أو استمالة المستخدمين النهائيين للدخول إلى مواقع ويب مقلدة. وتهدف بعض حملات التصيُّد إلى إقناع المستخدم إلى تثبيت برمجيات ضارة.

الاستدراج هو إعادة توجيه المستخدمين الغافلين إلى مواقع أو خدمات احتيالية، وذلك من خلال الاستيلاء في المعتاد على نظام أسماء النطاقات أو إفساده. ومن الممكن حدوث السطو على نظام أسماء النطاقات عندما يستخدم المهاجمون برامج ضارة من أجل إعادة توجيه الضحايا إلى موقع المهاجم بدلاً من الموقع المطلوب في البداية. ويتسبب إفساد نظام أسماء النطاقات في جعل خادم نظام أسماء النطاقات (أو وحدة حل التصديق) تستجيب بعنوان إنترنت خاطئ يحمل معه برمجيات ضارة. ويختلف التصيّد عن الاستدراج في أن الاستدراج ينطوي على تعديل إدخالات نظام أسماء النطاقات، في حين أن التصيّد يخدع المستخدمين بحملهم على إدخال معلومات شخصية.

---

[1] يمكن العثور على معلومات إضافية في التقرير المقدم من مجموعة المصالح الخاصة لانتهاك نظام أسماء النطاقات DNS في منتدى الاستجابة للحوادث وفرق الأمن, FIRST والذي يشتمل أيضًا على نصائح لفرق الاستجابة للحوادث في المؤسسات التي ربما تم التواصل معها بشكل مثمر في مراحل مختلفة من الاستجابة للحوادث لمختلف أساليب انتهاك نظام أسماء النطاقات DNS.
بالإضافة إلى ذلك، فقد قدمت شبكة سياسات الإنترنت والاختصاص القضائي (https://www.internetjurisdiction.net/) المزيد من الإرشادات حول هذه المعايير الخاصة بانتهاك نظام أسماء النطاقات DNS في "الآليات والأساليب والمعايير والأعراف التشغيلية."

[2] تقرير اللجنة الاستشارية للأمن والاستقرار في ICANN بسم SAC 115، القسم 2.1، الصفحات 12–13، بتاريخ 19 مارس 2021

البريد غير المرغوب عبارة عن بريد إلكتروني جماعي غير مرغوب، لم يمنح فيه المتلقي إذنًا أو تصريحًا للرسالة بأن ترسل إليه، ويتم فيه إرسال الرسالة ضمن مجموعة أكبر من الرسائل تضم جميعها بالأساس محتوى متطابقًا. ولا يعتبر البريد غير المرغوب ضمن انتهاك نظام أسماء النطاقات DNS إلا عندما يتم استخدامه كآلية تسليم وتنفيذ لواحد على الأقل من أنواع انتهاك نظام أسماء النطاقات DNS المذكورة أعلاه.

التزامات أمين السجل

القسم 3.18 من اتفاقية اعتماد أمناء السجلات

قبل سن وتشريع تعديلات انتهاك نظام أسماء النطاقات DNS، طالب القسم 3.18 أمناء السجلات بالاحتفاظ بتفاصيل جهة الاتصال ونشرها من أجل تلقي تقارير الانتهاك، بما في ذلك النشاط غير القانوني. وقد أوضح هذا الحكم أيضًا المتطلبات ذات الصلة بالتحري عن والرد على تقارير الانتهاكات التي تنطوي على أسماء مسجلة تحت رعاية أحد أمناء السجلات، إضافة إلى الدفاتر المرتبطة بذلك والتي يتعين على أمين السجل الاحتفاظ بها. وقد تم تعديل المتطلبات الواردة في اتفاقية اعتماد أمناء السجلات القسم 3.18 على نحو ما يلي:

المتطلبات ذات الصلة بنشر جهات اتصال الانتهاكات والاحتفاظ بها (اتفاقية اعتماد أمناء السجلات 3.18.1)

في حالة الإبلاغ عن انتهاكات[3]

لتسهيل تقديم التقارير من أي طرف يدعي وجود انتهاكات و/أو أنشطة غير قانونية، يجب على أمين السجل نشر عنوان بريد إلكتروني أو نموذج ويب يمكن الوصول إليه بسهولة على الصفحة الرئيسية لموقع أمين السجل على الويب[4]. ويجب ألا تطالب نماذج الويب بتسجيل دخول من أجل تقديم تقارير الانتهاكات.

والصفحة الرئيسية لأمين السجل التي تعرض بوضوح رابطًا يوصل إلى صفحة باسم "أبلغ عن انتهاك" أو "اتصل بنا" (والتي تشتمل بوضوح على جهة اتصال للتعامل مع الانتهاكات) وتتيح لمقدمي البلاغات تقديم التقارير بسهولة من الصفحة المرتبطة سوف يتم اعتبارها متوافقة.

تأكيد استلام تقارير الانتهاكات

بالإضافة إلى ذلك، يجب على أمين السجل تزويد مقدم بلاغ الانتهاكات بتأكيد على أن البلاغ قد تم استلامه. ويمكن إرسال تأكيد الاستلام هذا إلى مقدم بلاغ الانتهاك أو عرضه على الشاشة عند الانتهاء من التقديم إلى أمين السجل. ويجب أن يحتوي تأكيد الاستلام هذا على معلومات كافية تتيح لمقدم البلاغ القدرة على إيضاح أنه قد قدم البلاغ الخاص بالانتهاك. وعلى أقل تقدير، يجب أن يحدد تأكيد الاستلام أمين السجل والاسم (الأسماء) المسجلة المبلغ عنها، وتاريخ تقديم البلاغ.

جهات الاتصال لوكالات إنفاذ القانون

المتطلبات ذات الصلة بجهات الاتصال المخصصة لاستلام البلاغات المقدمة من جهات إنفاذ القانون (LEA) والجهات الأخرى ضمن اختصاص أمين السجل والمشار إليها في السابق في القسم 3.18.2 من اتفاقية اعتماد أمناء السجلات مدرجة الآن في اتفاقية اعتماد أمناء السجلات القسم 3.18.3؛ وهذه المتطلبات ما تزال كما هي بدون تغيير.

---

[3] أو لتجنب أي شك، فإن المتطلبات ذات الصلة بنشر عنوان البريد الإلكتروني لجهة اتصال الانتهاكات لدى أمين السجل ورقم الهاتف من خلال خدمات دليل بيانات التسجيل (RDDS) ما تزال بدون تغيير.

[4] ويجب أن يكون مكان موقع الويب هذا في نفس الرابط الموحد (URL) الذي يعرضه أمين السجل كقيمة بالنسبة لخانة "رابط URL لأمين السجل" عبر خدمات دليل بيانات التسجيل الخاصة به، وتوفيره إلى ICANN وإلى مشغل السجل من أجل النشر في خدمات دليل بيانات التسجيل الخاصة بمشغل السجل.

المتطلبات ذات الصلة باتخاذ إجراءات تخفيفية عند استلام البلاغات الموجبة لإقامة دعوى حول انتهاك نظام أسماء النطاقات DNS (اتفاقية اعتماد أمناء السجلات 3.18.2)

القسم 3.18.2 من اتفاقية اعتماد أمناء السجلات، حسب التعديلات التي أدخلت من خلال تعديلات انتهاك نظام أسماء النطاقات DNS، بات نصها الآن كما يلي:

> *عندما يكون لدى أمين السجل دليل موجب لإقامة دعوى بأن اسمًا مسجلاً تحت رعاية أمين السجل يجري استخدامه في انتهاك نظام أسماء النطاقات DNS، يجب على أمين السجل اتخاذ إجراء (إجراءات) فورية مناسبة للحد منها والتي تكون ضرورية بشكل معقول من أجل وقفها. أو قطع وإيقاف الاسم المسجل من أن يتم استخدامه في انتهاك نظام أسماء النطاقات DNS. قد يتفاوت الإجراء (الإجراءات) استنادًا إلى الظروف، مع الأخذ في الاعتبار سبب ومدى خطورة الضرر الناجم عن انتهاك نظام أسماء النطاقات DNS وإمكانية حدوث أضرار جانبية مرتبطة به.*

الدليل الموجب لإقامة دعوى

يجب أن يكون الدليل *موجبًا لإقامة دعوى*. وهذا يعني أن المعلومات المتاحة بالفعل أمام أمين السجل يجب أن تكون كافية لتمكين أمين السجل من اتخاذ قرار معقول بما إن كان الاسم المسجل يجري استخدامه في شكل واحد أو أكثر من أشكال انتهاك نظام أسماء النطاقات DNS أم لا. ونوصي بأن يقوم أمناء السجلات بإجراء مراقبة استباقية للأسماء المسجلة التي يرعونها من أجل تحديد انتهاك نظام أسماء النطاقات DNS المحتمل. وسوف يتفاوت تقييم أمين السجل للأدلة الموجبة لإقامة دعوى استنادًا إلى ظروف كل حالة على حدة.

الحصول على دليل موجب لإقامة الدعوى من طرف خارجي

نشر دار الأطراف المتعاقدة (CPH) إرشادات للمساعدة في تقديم تقارير انتهاك مكتملة وموجبة لإقامة دعوى إلى أمناء السجلات (والمشار إليها بلفظ إرشادات دار الأطراف المتعاقدة). وتصف إرشادات دار الأطراف المتعاقدة الدليل الذي يميل إلى جعل تقارير الانتهاك موجبة لإقامة الدعوى. على سبيل المثال، لقطة شاشة توضح محاولة تصيُّد مع توضيح ما يستهدفه التصيُّد (مؤسسة مالية على سبيل المثال)؛ ورابط URL الكامل الذي يوجد به الانتهاك، (على سبيل المثال، example[.]tld/badpage[.]html)[5]. نوصي مقدمي بلاغات الانتهاكات بمراجعة متابعة إرشادات دار الأطراف المتعاقدة، وتزويدنا بأكبر قدر من المعلومات داخل تقاريرهم، من أجل تمكين أمين السجل من إجراء تحريات حول انتهاك نظام أسماء النطاقات DNS المحتمل.

وفي الحالات التي يتلقى فيها أمين سجل تقرير انتهاك لا يحتوي على جميع المعلومات اللازمة لكي يعتبر دليلاً موجبًا لإقامة دعوى بخصوص انتهاك نظام أسماء النطاقات DNS، يجب على أمين السجل التحري حسب القسم 3.18 من اتفاقية اعتماد أمناء السجلات. وفي بعض الحالات، قد يكون لأمين السجل وصولاً إلى المعلومات التي لم يتم تقديمها من جانب مقدم بلاغ الانتهاك لكنها ضرورية أو مفيدة في تحديد أن الاسم المسجل يجري استخدامه من أجل انتهاك نظام أسماء النطاقات DNS. وفي تلك الحالات، يجب على أمين السجل مراعاة المعلومات التي يمكنه الوصول إليها بشكل معقول وتكون ذات صلة بالتحقيقات (على سبيل المثال، خوادم الاسم، ومعلومات الحساب والنشاط والمحتويات في صفحة الويب الأولية على أقل تقدير أو في رابط URL المحدد في تقرير الانتهاك، في حالة تقديمه).

بعد الدليل الموجب لإقامة دعوى، يجب اتخاذ إجراء فوري

عند الحصول على دليل موجب لإقامة دعوى، يجب على أمين السجل اتخاذ إجراء (إجراءات) *فورية* مناسبة *للحد منها والتي* تكون ضرورية بشكل معقول من أجل وقف أو قطع الاسم المسجل من أن يتم استخدامه في انتهاك نظام أسماء النطاقات DNS. ولتحديد وتقرير إجراءات الحد من الانتهاكات التي تكون فورية ومناسبة، ينظر أمين السجل في الظروف النوعية

[5] رابط URL هذا موضع في نسق معروف باسم "رابط URL المثبط". ورابط URL المثبط يمكن للعين البشرية قراءته لكن من غير الممكن النقر فوقه. ومن ثم، إذا قمت أنت أو متلقي تقرير الانتهاك بالنقر فوق رابط URL بالخطأ، فلن يقوم بتوجيهك أو توجيه المتلقي إلى موقع قد يكون ضارًا.

للحالة، والتي قد تشتمل على الموازنة بين نطاق وحدة الضرر الناجم عن انتهاك نظام أسماء النطاقات DNS في مقابل احتمالية الضرر الجانبي المرتبط بها.

الأضرار الجانبية أو العرضية عبارة عن اعتبار هام بشكل خاص في حالة استخدام اسم نطاق مشروع أو حميد ليكون متجهًا من أجل انتهاك نظام أسماء النطاقات DNS دون علم أو موافقة المسجل. وغالبًا ما يشار إلى ذلك الأمر بأنه "النطاق المخترق" وفي بعض الأحيان يكون نتيجة نظام منتهك لإدارة محتوى موقع الويب. وفي حالات الاختراق هذه، فإن التعليق المباشر للنطاق من جانب أمين السجل أو مشغل السجل قد لا يكون هو الحل المناسب، حيث سيمنع التعليق الوصول إلى جميع المحتويات المشروعة بالإضافة إلى جعل أي بريد إلكتروني أو خدمات أخرى مرتبطة به مع النطاق محظورة[6]. وهذا هو الحال أيضًا عندما يكون انتهاك نظام أسماء النطاقات DNS مرتبطًا بمستوى ثالث أو بنطاق فرعي. ولا يمكن لأمناء السجلات والسجلات التصرف إلا في المستوى مستوى نطاقات المستوى الثاني. ومن ثم، إذا قاموا بتعليق نطاق المستوى الثاني، فسوف يتم تعليق نطاقات المستوى الثالث أيضًا، وليس فقط النطاق المرتبط بانتهاك نظام أسماء النطاقات DNS. وفي هذه المواقف، قد يختار أمين السجل توفير إشعار إلى المسجل أو مشغل الموقع أو مضيف الويب أو إليهم جميعًا.

ما الذي يضفي على الإجراء صفة الفورية

وفقًا لما أوضحنا أعلاه، فإن إجراء التخفيف المناسب لوقف أو قطع حالة من حالات انتهاك نظام أسماء النطاقات DNS سوف يتفاوت استنادًا إلى الظروف النوعية. وبالتالي، فإن المقدار الزمني المناسب للتحري واتخاذ إجراء سوف يتفاوت، الأمر الذي يجعل من المستحيل تحديد مقدار زمني محدد لأي إجراء يجب اعتباره "فوريًا". وعوضًا عن ذلك، يجب على أمناء السجلات إظهار اهتمام مستمر بادعاءات الأسماء المرعية التي يجري استخدامها في انتهاك نظام أسماء النطاقات DNS. ويجب أن يكون الاهتمام متساوقًا مع الضرر المحتمل الذي يتسبب فيه انتهاك نظام أسماء النطاقات DNS للضحايا.

وطبقًا لذلك، ردًا على أي استعلام مقدم من إدارة الامتثال التعاقدي في ICANN، سوف يكون أمناء السجلات مطالبون بتفسير الكيفية التي كانت بها الإجراءات فورية بالنظر إلى الظروف النوعية. وسوف تقوم إدارة الامتثال التعاقدي في ICANN حينها بمراجعة التفسير والظروف ذات الصلة من أجل اتخاذ قرار قائم على كل حالة على حدة فيما يخص ما إن كانت الإجراءات فورية بشكل معقول أم لا. علمًا بأن الأطر الزمنية في الأمثلة المشمولة في هذه المشورة ليست متطلبات تعاقدية، لكنها توضيحية وبيانية فقط. وأمين السجل الذي يستغرق وقتًا أطول في التحري واتخاذ الإجراءات ضد قضية مشابهة للأمثلة لن يكون بالضرورة دليلاً على عدم الامتثال. وعلى النقيض من ذلك، قد تتطلب الظروف والحالات الأخرى من أمين السجل التصرف بسرعة أكبر، مثل حالات انتهاك نظام أسماء النطاقات DNS التي تحمل في طياتها احتمالية التسبب في ضرر وشيك للمستخدمين النهائيين. من المتوقع أن يقوم أمين السجل بالتحري واتخاذ إجراء بأسرع ما يمكن بعد محاولة أمين السجل المعقولة تأكيد حالة انتهاك نظام أسماء النطاقات DNS.

تجميع الأمر - أمثلة الامتثال لأمناء السجلات

توضح الأمثلة التالية إجراءات الحد من الانتهاكات المعقولة والفورية والتي تم اتخاذها من أجل وقف الاسم المسجل من استخدمها من أجل انتهاك نظام أسماء النطاقات DNS (السيناريو الأول) ووقف مسيرة انتهاك نظام أسماء النطاقات DNS فيما يتصل بالاسم المسجل (السيناريو الثاني). وتحتوي هذه السيناريوهات على ظروف فعلية ونوعية. وفي ظل الظروف المختلفة، يجوز لكل واحد من أمناء السجلات اتخاذ إجراءات مختلفة وضمن إطار زمني مختلف من أجل وقف أو قطع حالات انتهاك نظام أسماء النطاقات DNS الفردية. وفي جميع الأحوال، يجب أن تكون لأمناء السجلات القدرة على إيضاح أن أي أسلوب متخذ يتوافق مع المتطلبات ذات الصلة في القسم 3.18 من اتفاقية اعتماد أمناء السجلات.

[6] المزيد من المعلومات حول الأضرار الجانبية واعتبارات التناسبية عند التصرف في مستوى نظام أسماء النطاقات متوفرة في منشور شبكة سياسات الإنترنت والاختصاص القضائيبعنوان "مجموعة الأدوات: الإجراء في مستوى نظام أسماء النطاقات من أجل التعامل مع الانتهاكات."

السيناريو الأول: يتلقى أمين السجل تقرير انتهاك كامل وموجب لإقامة دعوى يزعم بأن اسمًا مسجلاً تحت رعاية أمين السجل يجري استخدامه في أعمال التصيُّد. ويشتمل التقرير على أدلة بأن رابط URL يحتوي على الاسم المسجل تحت رعاية أمين السجل يجري إرساله عن طريق البريد الإلكتروني أو رسائل SMS مقدمًا نفسه على أنه بنك كبير ويطالب المتلقين بإلغاء قفل حساباتهم. يبدأ أمين السجل تحريات للنظر في جميع المعلومات ذات الصلة المشمولة في تقرير الانتهاكات. وتميط تحريات أمين السجل اللثام عن أن الاسم المسجل ليس لديه موقع ويب متاح للجميع وأنه يعرض فقط رابط URL مباشرًا مع ما يبدو أنه شاشة تسجيل دخول لبنك كبير. ونفس رابط URL هو الرابط الذي يجري إرساله عن طريق البريد الإلكتروني أو الرسائل القصيرة SMS. ويرى أمين السجل أيضًا أن العميل جديد وأن الاسم المسجل تم تسجيله قبل ذلك بخمسة أيام.

الإجراءات المناسبة للحد من الانتهاكات: ويخلص أمين السجل في النهاية وبشكل معقول إلى أن الاسم المسجل يجري استخدامه من أجل انتهاك نظام أسماء النطاقات DNS ويقوم بوقف انتهاك نظام أسماء النطاقات DNS عن طريق تعليق الاسم المسجل، بتطبيق clientHold أو رمز حالة (EPP) بروتوكول التزويد الموسّع[7]. وتحدث التحريات وعملية الحد من المخاطر في غضون يومي عمل رسميين اعتبارًا من استلام بلاغ الانتهاك. ويجوز لأمين السجل أيضًا أن يقرر تطبيق قف تحويل للاسم المسجل من أجل منع المسجل من محاولة التملص من إجراء الحد من الانتهاك واستئناف استخدام اسم النطاق لانتهاك نظام أسماء النطاقات DNS، طالما أن أمين السجل يتوافق مع المتطلبات المعمول بها والمنصوص عليها في سياسة نقل الملكية في ICANN.

السيناريو الثاني: يتلقى أمين السجل تقرير انتهاك كامل وموجب لإقامة دعوى يزعم بأن اسمًا مسجلاً تحت رعاية أمين السجل، وهو autobrand.tld، يجري استخدامه في أعمال التصيُّد. ويشتمل تقرير الانتهاك على أدلة بأن رابط URL محدد يجري استخدامه في أعمال التصيُّد. يجري أمين السجل تحريات، مراجعًا لجميع المعلومات ذات الصلة المشمولة في تقرير الانتهاكات بالإضافة إلى المعلومات المتاحة بالفعل والمتاحة بشكل معقول لأمين السجل.

وتؤكد التحريات أن رابط URL في تقرير الانتهاك يجري استخدامه في أعمال التصيُّد. كما تكشف التحريات عن أن رابط URL ينتمي إلى نطاق فرعي (city.autobrand.tld)، ويبدو أن يُستخدم من خلال أحد الحاصلين على حق امتياز. ويقر أمين السجل بأن الاسم المسجل autobrand.tld تم تسجيله منذ ثلاث سنوات كما أنه يحتوي على مجموعة قوية من المحتويات لعقد امتياز في تجارة السيارات. كما أن لأمين السجل القدرة على تأكيد أن الاسم المسجل يُستخدم من أجل رسائل البريد الإلكتروني الرسمية لشركة Autobrand والنطاقات الفرعية للعديد من الحاصلين على حق الامتياز.

الإجراءات المناسبة للحد من الانتهاكات: يخلص أمين السجل في النهاية وبشكل معقول إلى أن الاسم المسجل يجري استخدامه من أجل انتهاك نظام أسماء النطاقات DNS، ولكن هذا على الأرجح نتيجة اختراق النطاق وأن المسجل لا يستخدم الاسم المسجل على دراية من أجل انتهاك نظام أسماء النطاقات DNS. ويقوم أمين السجل بتقييم الأضرار الجانبية المحتملة التي يمكن أن يحدثها إيقاف أو تعليق اسم النطاق، ويخلص بشكل معقول إلى أنه ليس الإجراء المناسب للحد من الضرر في هذا الوقت. وعوضًا عن ذلك، يقوم أمين السجل بقطع انتهاك نظام أسماء النطاقات DNS من خلال إشعار شركة Autobrand، وهي مسجل نطاق autobrand.tld، مطالبًا بأن تقوم بإزالة وإلغاء محتوى التصيُّد بحلول تاريخ محدد يقرره أمين السجل بشكل معقول. وتحدث التحريات وعملية الحد من المخاطر في غضون ثلاثة أيام عمل رسمية اعتبارًا من استلام تقرير الانتهاك.

المتطلبات ذات الصلة بحفظ السجلات وتوفيرها إلى ICANNالمتطلبات ذات الصلة بتوثيق وتوفير السجلات ذات الصلة بتسلم تقارير الانتهاك والرد عليها والمشار إليها في السابق في القسم 3.18.3 من اتفاقية اعتماد أمناء السجلات مدرجة الآن في اتفاقية اعتماد أمناء السجلات القسم 3.18.4؛ وهذه المتطلبات ما تزال كما هي بدون تغيير. كما تسري هذه المتطلبات على الرد على تقارير انتهاك نظام أسماء النطاقات DNS بموجب القسم 3.18.2.

[7] انقر هنا للحصول على مزيد من المعلومات من ICANN حول رموز حالة بروتوكول التزويد الموسّع.

التزامات مشغل السجل

القسم 4، المواصفة 6 من اتفاقية السجل

تشترط المواصفة 6، القسم 4 من اتفاقية السجل نشر وتزويد ICANN بتفاصيل الاتصال الخاصة بالتعامل مع الانتهاكات ذات الصلة بالتصرفات الضارة في نطاق المستوى الأعلى (TLD). كما أنها تشتمل على متطلبات مرتبطة بإزالة سجلات الملصق المعزولة عند استخدامها فيما يتصل بالتصرفات الضارة. وقد تم تعديل المتطلبات الواردة في هذه المواصفة على نحو ما يلي:

المتطلبات ذات الصلة بنشر جهات اتصال الانتهاكات والاحتفاظ بها (اتفاقية السجل المواصفة 6، القسم 4.1)

مكان الإبلاغ عن انتهاكات
لتسهيل تقديم التقارير من أي طرف يدعي وجود تصرفات ضارة في نطاق المستوى الأعلى، بما في ذلك انتهاك نظام أسماء النطاقات DNS، يجب على مشغل السجل نشر عنوان بريد إلكتروني أو نموذج ويب، وعنوان مراسلة وجهة اتصال أولية من أجل التعامل مع تلك التقارير.

الصفحة الرئيسية لمشغل السجل التي تعرض بوضوح رابطًا يوصل إلى صفحة باسم "أبلغ عن انتهاك" أو "اتصل بنا" (والتي تشتمل بوضوح على جهة اتصال للتعامل مع الانتهاكات) حيث يكون تقديم البلاغات بدون أي عوائق فإنها تعتبر متوافقة.

تأكيد استلام تقارير الانتهاكات
وعند الاستلام، يجب على مشغل السجل تزويد مقدم بلاغ الانتهاكات بتأكيد على أن البلاغ قد تم استلامه. ويمكن إرسال تأكيد الاستلام هذا إلى مقدم بلاغ الانتهاك أو عرضه على الشاشة عند الانتهاء من التقديم إلى مشغل السجل. ويجب أن يحتوي تأكيد الاستلام هذا على معلومات كافية تتيح لمقدم البلاغ القدرة على إيضاح تقديم البلاغ الخاص بالانتهاك. وعلى أقل تقدير، يجب أن يحدد تأكيد الاستلام مشغل السجل والاسم (الأسماء) المسجلة المبلغ عنها، وتاريخ تقديم البلاغ.

المتطلبات ذات الصلة باتخاذ إجراءات تخفيفية عند استلام البلاغات الموجبة لإقامة دعوى حول انتهاك نظام أسماء النطاقات DNS (اتفاقية السجل المواصفة 6، القسم 4.2)

القسم 4.2 من المواصفة 6 وما جرى عليه من تعديلات بموجب تعديلات انتهاك نظام أسماء النطاقات DNS، بات نصه الآن على نحو ما يلي:

> *متى ما قرر مشغل سجل بشكل معقول وعلى أساس الدليل الموجب لإقامة الدعوى بأن اسم نطاق مسجل في نطاق المستوى الأعلى TLD يجري استخدامه في انتهاك نظام أسماء النطاقات DNS، فيجب على مشغل السجل أن يتخذ على الفور الإجراء (الإجراءات) المناسبة للحد منها والتي تكون ضرورية بشكل معقول من أجل الإسهام في وقف أو حتى منع اسم النطاق من استخدامه في انتهاك نظام أسماء النطاقات DNS. ويشتمل ذلك الإجراء (الإجراءات) على الأقل على ما يلي: (1) إحالة النطاقات التي يجري استخدامها في انتهاك نظام أسماء النطاقات DNS بالإضافة إلى الأدلة ذات الصلة إلى أمين السجل الراعي؛ أو (2) اتخاذ إجراء مباشر من جانب مشغل السجل، متى ما رأى مشغل السجل ذلك مناسبًا. قد يتفاوت الإجراء (الإجراءات) استنادًا إلى ظروف كل حالة، مع الأخذ في الاعتبار خطورة الضرر الناجم عن انتهاك نظام أسماء النطاقات DNS وإمكانية حدوث أضرار جانبية مرتبطة به.*

الدليل الموجب لإقامة دعوى

يجب أن يكون الدليل *موجبًا لإقامة دعوى*. وهذا يعني أن المعلومات المتاحة بالفعل أمام مشغل السجل يجب أن تكون كافية لتمكين مشغل السجل من اتخاذ قرار معقول بما إن كان الاسم المسجل يجري استخدامه في شكل واحد أو أكثر من أشكال انتهاك نظام أسماء النطاقات DNS أم لا. ويجوز لمشغلي السجلات الحصول على أدلة موجبة لإقامة دعوى من خلال مراجعة المعلومات التي يمكنهم الوصول إليها بشكل معقول ومستقل، سواء كان فيما يتصل ببلاغ عن انتهاك أو في إطار جهودهم الخاصة بموجب المواصفة 11(3)(ب) لاتفاقية السجل عن طريق إجراء تحليل فني من أجل تحديد النطاقات التي يجري استخدامها في انتهاك نظام أسماء النطاقات DNS. كما يمكن عرض الأدلة الموجبة لإقامة دعوى على مشغل السجل عن طريق طرف خارجي مثل وكالات إنفاذ القانون، أو المصادر المعتمدة أو المقررة لدى مشغل السجل أو أي طرف أو مصدر آخر. ونحن نوصي مقدمي بلاغات الانتهاكات بتوفير أكبر قدر ممكن من المعلومات من أجل الإسهام في ضمان حصول مشغل السجل على المعلومات الكافية من أجل إجراء تحريات حول انتهاك نظام أسماء النطاقات DNS المحتمل. ولتجنب حدوث أي شك، أي بلاغ بانتهاكات يعتبر غير مكتمل من جانب مشغل السجل من الممكن اعتباره موجبًا لإقامة الدعوى إذا كان لمشغل السجل القدرة على الوصول إلى معلومات كافية من أجل إجراء معقول لتحريات من أجل الوقوف على ما إن كان الاسم المسجل يُستخدم في انتهاك نظام أسماء النطاقات DNS.

بعد الدليل الموجب لإقامة دعوى، يجب اتخاذ إجراء فوري

عند الحصول على دليل موجب لإقامة دعوى، يجب على مشغل السجل اتخاذ إجراء (إجراءات) فورية مناسبة للحد منها والتي تكون ضرورية بشكل معقول من أجل وقف أو حتى قطع استخدام اسم النطاق في انتهاك نظام أسماء النطاقات DNS. ولتحديد وتقرير الإجراءات المناسبة، ينظر مشغل السجل في الظروف النوعية للحالة، والتي قد تشتمل على الموازنة بين نطاق الضرر الناجم والمخالفة الحادثة عن انتهاك نظام أسماء النطاقات DNS في مقابل احتمالية الضرر الجانبي المرتبط بها. كما أن أهمية الأضرار الجانبية في موقف النطاقات المخترقة الموصوف أعلاه لأمناء السجلات ينطبق بالتساوي على السجلات.

وسوف ينظر مشغل السجل أيضًا فيم إن كان أمين السجل الراعي أو طرف آخر أو كليهما هما الأطراف الأكثر تأهلاً لمراجعة واتخاذ إجراءات الحد من الانتهاكات المناسبة والمتناسبة. على سبيل المثال، لاسم مسجل فردي يجري استخدامه في انتهاك نظام أسماء النطاقات DNS، قد يكون أمين السجل هو الأفضل في مراجعة معالجة انتهاك نظام أسماء النطاقات DNS مع عميله. وبالمثل، في حالة الأنظمة المخترقة، فإن صاحب الاسم المسجل أو موفر الاستضافة القائم على توفير الوصول الإداري إلى الأنظمة المتضررة قد يكون الأقدر على التعامل مع المشكلات، ويجب على مشغل السجل إحالتها إلى أمين السجل أولاً، حيث إن تعليق النطاق من خلال تطبيق clientHold أو serverHold قد يتسبب في ضرر جانبي على المحتوى الحميد أو المشروع. وعلى الجانب الآخر، قد يكون مشغل السجل هو الطرف الأنسب في التعامل مع التهديدات الكبيرة التي تنتشر بين العديد من أصحاب الأسماء المسجلة أو أمناء السجلات، مثل خوارزميات استخراج النطاقات المستخدمة من أجل نشر وتوزيع شبكات بوت نت.

وإجراءات التخفيف المتخذة على الفور يجب أن تكون ضرورية بشكل معقول من أجل تحقيق أحد النتائج التالية: *الإسهام في وقف* أو *قطع* الاسم المسجل من أن يتم استخدامه في انتهاك نظام أسماء النطاقات DNS. وعلى الأقل، يجب على مشغل السجل أيّ ما يلي:

1) *الإبلاغ* عن الاسم (الأسماء) المسجلة *وتوفير* الدليل ذي الصلة إلى أمين (أمناء) السجلات الرعاة
2) *أو اتخاذ إجراء مباشر* حيال الاسم (الأسماء) المسجلة متى ما رأى مشغل السجل هذا الإجراء المباشر مناسبًا.

ما الذي يضفي على الإجراء صفة الفورية

وفقًا لما أوضحنا أعلاه بالنسبة لأمناء السجلات، فإن الإجراء المناسب الذي يجب اتخاذه من أجل التخفيف أو قطع حالة من حالات انتهاك نظام أسماء النطاقات DNS سوف يتفاوت استنادًا إلى الظروف النوعية.
وبالتالي، فإن المقدار الزمني المناسب للتحري واتخاذ إجراء مناسب سوف يتفاوت، الأمر الذي يجعل من المستحيل تحديد مقدار زمني محدد لأي إجراء يجب اعتباره "فوريًا". وعوضًا عن ذلك، يجب على مشغلي السجلات إظهار اهتمام مستمر

بادعاءات الأسماء المرعية التي يجري استخدامها في انتهاك نظام أسماء النطاقات DNS. ويجب أن يكون الاهتمام متساوقًا مع الضرر المحتمل الذي يتسبب فيه انتهاك نظام أسماء النطاقات DNS للضحايا.

وطبقًا لذلك، وردًا على أي استعلام مقدم من إدارة الامتثال التعاقدي في ICANN، سوف يكون مُشغلو السجلات مطالبون بتفسير الكيفية التي كانت بها الإجراءات فورية بالنظر إلى الظروف النوعية. وسوف تقوم إدارة الامتثال التعاقدي في ICANN حينها بمراجعة التفسير والظروف ذات الصلة من أجل اتخاذ قرار قائم على كل حالة على حدة فيما يخص ما إن كانت الإجراءات فورية أم لا. علمًا بأن الأطر الزمنية في الأمثلة المشمولة في هذه المشورة ليست متطلبات تعاقدية، لكنها توضيحية وبيانية فقط. ومشغل السجل الذي يستغرق وقتًا أكثر في حالة خاصة لن يكون بالضرورة إشارة على عدم الالتزام. وعلى النقيض من ذلك، قد تتطلب الظروف والحالات الأخرى من مشغل السجل التصرف بسرعة أكبر، مثل حالات التهديدات كبيرة الحجم التي تحمل في طياتها احتمالية التسبب في ضرر وشيك لعدد كبير من المستخدمين النهائيين. من المتوقع أن يقوم مشغل السجل بالتحري واتخاذ إجراء بأسرع ما يمكن بعد محاولة مشغل السجل المعقولة تأكيد حالة انتهاك نظام أسماء النطاقات DNS.

توضح الأمثلة التالية إجراءات التخفيف المعقولة التي تم اتخاذها على الفور من أجل الإسهام في وقف الاسم المسجل من استخدامه في انتهاك نظام أسماء النطاقات DNS (السيناريو الثاني) والإسهام في منع وقطع مسيرة انتهاك نظام أسماء النطاقات DNS فيما يتعلق بالاسم المسجل (السيناريو الأول والثالث). وتحتوي هذه السيناريوهات على ظروف فعلية ونوعية. وفي ظل الظروف المختلفة، يجوز لكل واحد من مشغلي السجلات اتخاذ إجراءات مختلفة وضمن فترات زمنية مختلف من أجل الإسهام في وقف أو قطع حالات انتهاك نظام أسماء النطاقات DNS الفردية. وفي جميع الأحوال، يجب أن تكون لمشغلي السجلات القدرة على إيضاح أن أي أسلوب متخذ يتوافق مع المتطلبات ذات الصلة في القسم 4.2 في المواصفة 6 من اتفاقية السجل.

قسم 3(ب)، المواصفة 11 من اتفاقية السجل

تم تعديل هذا القسم لكي يحل محل المصطلح المعرف لانتهاك نظام أسماء النطاقات DNS المنصوص عليه في التعديلات التي أدخلت على المواصفة 6، القسم 4، من أجل "التهديدات الأمنية".

تجميع الأمر - أمثلة امتثال مشغلي السجلات

السيناريو الأول: مشغل سجل يتلقى إشعارًا من اتحاد ائتماني (مثال على الاتحادات الائتمانية) مثل نموذج ويب الانتهاك الخاص به بأن شخصًا قام بتسجيل النطاق <loginexamplecreditunion[.]TLD> منذ ستة أيام واتحاد الائتمان يزعم بأن النطاق متورط في أعمال تصيُّد. ويقدم اتحاد الائتمان لقطة شاشة توضح صفحة ويب على النطاق تقوم بجمع بيانات إثبات الهوية المستخدمة في تسجيل الدخول.

الإجراءات المناسبة للحد من الانتهاكات: ويقوم مشغل السجل بمعالجة البلاغ ومراجعته في غضون يومي عمل متبعًا في ذلك ما لديه من إجراءات داخلية. وعند إجراء هذه التحريات، قرر مشغل السجل بشكل معقول بأن الاسم المسجل كان قيد الاستخدام في انتهاك نظام أسماء النطاقات DNS. ومن ثم يقوم مشغل السجل بقطع ووقف مسار انتهاك نظام أسماء النطاقات DNS عن طريق إشعار أمين السجل الراعي وتزويده بجميع المعلومات ذات الصلة. ويقوم مشغل السجل بتضمين طلب مقيد بفترة زمنية لأمين السجل من أجل التحري واتخاذ الإجراءات الضرورية بشكل معقول من أجل الحد من الانتهاك لوقف أو قطع انتهاك نظام أسماء النطاقات DNS. وبحلول الموعد النهائي المحدد، يكون مشغل السجل قادرًا على تأكيد أن أمين السجل قام بتعليق عمل الاسم المسجل من خلال تطبيق رمز حالة بروتوكول التزويد الموسّع clientHold.

السيناريو الثاني: تلجأ وكالات إنفاذ القانون إلى مشغل سجل وتقدم له أدلة على أن سلسلة من النطاقات تنخرط أو سوف تتورط في خوارزمية استخراج النطاقات المرتبطة بشبكة بوت نت. وتشتمل شبكة بوت نت على أسماء مسجلة حالية، ولكن على الأكثر فهي نطاقات لم يتم تسجيلها إلى الآن.

الإجراءات المناسبة للحد من الانتهاكات: وفي غضون ست ساعات من إجراء مشغل السجل لتحرياته وتأكيد وجود انتهاك لنظام أسماء النطاقات DNS بشكل معقول، يسهم مشغل السجل في إيقاف انتهاك نظام أسماء النطاقات DNS من خلال اتخاذ الإجراءات التي توجه بها وكالات إنفاذ القانون أو توافق عليها. وفي هذه الحالة، فقد وافق مشغل السجل على أنه بالنسبة للأسماء المسجلة ذات الصلة، سوف يقوم السجل بتفويض خادم (خوادم) اسم مختلفة (على سبيل المثال إعادة توجيه خوادم الاسم أو الإيقاع بها) بطلب من وكالات إنفاذ القانون. كما يقوم مشغل السجل مباشرة بإنشاء النطاقات بالنسبة لتلك النطاقات غير المسجلة في السابق والمرتبطة بشبكة بوت نت حسب طلب وكالات إنفاذ القانون. ومع ملاحظة أن إنشاء النطاقات من خلال مشغل السجل يتطلب في المعتاد تصريحًا من خلال الإعفاء من الرد الأمني في ICANN أو (SRW[8]). وسوف يطلب مشغل السجل أيضًا في الوقت المناسب الحصول على إعفاء تعاقدي. ويشار أيضًا على الرغم من ذلك إلى أن الإعفاء من الرد الأمني من الممكن أيضًا تطبيقه بأسرع ما يمكن من الناحية العملية بعد التحقق، ويجوز لمنظمة ICANN الرد بإعفاء بأثر رجعي إن كان مناسبًا، بحيث لا يتم تأخير الدعم المقدم من تشغلي وكالات إنفاذ القانون[9].

السيناريو الثالث: وفي إطار إجراء مشغل السجل لتحليل فني بحثًا عن انتهاك نظام أسماء النطاقات DNS بموجب المواصفة 11(3)(ب)، فإنه يكتشف أن صفحة فرعية للنطاق يجري استخدامها في توزيع البرمجيات الضارة في حين أن بقية الموقع على النطاق تبدو بأنها محتوى مشروع أو ليس منه ضرر. كما تم تسجيل النطاق لمدة ثلاث سنوات.

الإجراء المناسب للحد من الانتهاكات: وفي غضون ثلاث ساعات من معرفة وتحديد أن الاسم المسجل يجري استخدامه من أجل انتهاك نظام أسماء النطاقات DNS وأنه مخترق، يسهم مشغل السجل في قطع مسار انتهاك نظام أسماء النطاقات DNS من خلال إبلاغ وتوفير جميع المعلومات ذات الصلة إلى أمين السجل الراعي مع تقديم طلب مقيد زمنيًا من أجل إجراء من جانب أمين السجل للرد على البلاغ. بعد ذلك يقوم أمين السجل بإشعار المسجل مباشرة، وهو ما يؤدي إلى حل المشكلة من خلل تحديث نظام إدارة المحتوى الخاص به لإزالة البرمجيات الضارة.

تحريات منظمة ICANN حول الامتثال مع القسم الجديد 3.18.2 في اتفاقية اعتماد أمناء السجلات والقسم 4.2 من المواصفة 6 في اتفاقية السجل

ما الذي يمكن أن يمثل ردًا متوافقًا وكاملاً وبالأدلة الكافية؟ سوف تقوم إدارة الامتثال التعاقدي في ICANN بإنفاذ المتطلبات الموضحة في هذه المشورة من خلال معالجة الشكاوى الخارجية ومن خلال المراقبة الاستباقية وأنشطة التدقيق. فعندما تتلقى إدارة الامتثال التعاقدي في ICANN شكوى، فسوف تقوم بمراجعة أي من الأدلة المقدمة من خلال مقدم البلاغ بالإضافة إلى أي معلومات ذات صلة متاحة من أجل تحديد ما إن كانت حالة امتثال من الواجب البدء فيها أم لا مع أمين السجل أو مشغل السجل المعني. وفي حالة غياب الأدلة الكافية التي تدعم وتؤيد الادعاء بوجود انتهاك نظام أسماء النطاقات DNS، سوف تقوم إدارة الامتثال التعاقدي في ICANN بإغلاق القضية باعتبارها غير صحيحة. فعلى سبيل المثال لا الحصر، سوف تنظر هذه

[8] يمكن الاطلاع على معلومات حول الإعفاءات من الرد الأمني على هذه الصفحة.

[9] للحصول على مزيد من المعلومات حول الطريقة التي يمكن للسجلات العمل بها مع جهات إنفاذ القانون وICANN من أجل التعامل مع خوارزميات استخراج النطاقات، برجاء الاطلاع على "إطار عمل حول خوارزميات استخراج النطاقات المرتبطة بالبرمجيات الضارة وشبكات بوت نت"، التي نشرتها مجموعة عمل السلامة العامة في اللجنة الاستشارية الحكومية ومجموعة أصحاب المصلحة لسجلات نطاقات gTLD.

المراجعة فيم إن كانت المعلومات المتاحة بالفعل أمام أمين السجل الراعي مباشرة أو من خلال موزع فرعي، أو مشغل السجل، حسبما يقتضي الحال، كافية من أجل الوقوف بشكل معقول على ما إن كان الاسم المسجل يجري استخدامه في شكل أو أكثر من أشكال انتهاك نظام أسماء النطاقات DNS. كما ستنظر المراجعة أيضًا فيم إن كان كانت هناك أي معلومات إضافية مقدمة من الطرف مقدم البلاغ ردًا على طلبات أمين السجل أو مشغل السجل من أجل الحصول على معلومات أو أدلة إضافية.

وعلاوة على ذلك، متى ما كان الأمر منطبقًا وذي صلة بالحالة الخاصة، سوف تقوم إدارة الامتثال التعاقدي في ICANN بما يلي: (1) مراجعة البيانات ذات الصلة والقابلة للوصول إليها عمومًا والمعروضة من خلال خدمات دليل بيانات التسجيل، على سبيل المثال تاريخ الإنشاء وحالة (حالات) بروتوكول التزويد المرن أو معلومات خوادم الاسم؛ و(2) إجراء عمليات بحث DNS من أجل معرفة ما إن كانت الأسماء المسجلة المبلغ عنها تنحل إلى عناوين في نظام أسماء النطاقات أم لا. كما يجوز لإدارة الامتثال التعاقدي في ICANN إجراء عمليات البحث الخاصة بها ومراجعة المعلومات الإضافية ذات الصلة حول اسم مسجل خاص ثمة ادعاء بأنه متورط في انتهاكات لنظام أسماء النطاقات DNS.

عند البدء في قضية امتثال مع أحد أمناء السجلات ومشغل السجل بموجب القسم 3.18.2 من اتفاقية اعتماد أمناء السجلات أو القسم 4.2 من المواصفة 6 في اتفاقية السجل، على التوالي، سوف توفر إدارة الامتثال التعاقدي في ICANN قائمة مفهرسة بجميع المعلومات والسجلات اللازمة لتقييم الامتثال وارتباطه بالاسم (الأسماء) المسجلة وأشكال انتهاك نظام أسماء النطاقات DNS المبلغ عنها. وردًا على حالة امتثال، سوف يكون من المتوقع بالنسبة لأمين السجل ومشغل السجل على أقل تقدير ما يلي:

- شرح طريقة وسبب توصل أمين السجل أو مشغل السجل إلى قرار بأن الدخل المتحصل عليه لم يكن موجبًا لإقامة الدعوى، متى ما كان ذلك منطبقًا. على سبيل المثال، يجوز لأمين السجل أن يوضح أنه وبعد مراجعة المعلومات والسجلات المقدمة من الطرق مقدم البلاغ، ومن خلال تحرياته بأن أمين السجل لم يكن قادرًا على توثيق أن انتهاك نظام أسماء النطاقات DNS كان يجري فيما يتصل بالاسم (الأسماء) المسجلة المبلغ عنها. ويجوز لإدارة الامتثال التعاقدي في ICANN أن تطلب من أمين السجل أو مشغل السجل توضيح أي تضاربات واضحة بين التفسير المقدم وأي معلومات وبيانات حصلت عليها إدارة الامتثال التعاقدي في ICANN خلال عملية توثيق الشكوى.
- توفير تفسير تفصيلي تدعمه السجلات ذات الصلة لكل من الإجراءات التخفيفية النوعية المتخذة، وموعد اتخاذ تلك الإجراءات، وكيف تم اعتبار ما تم اتخاذه من إجراءات فورية وضرورية بشكل معقول من أجل وقف أو قطع أو الإسهام في قطع أو وقف الانتهاكات، وارتباط ذلك بالظروف النوعية للحالة (بما في ذلك أي تفسير منطبق يتعلق بعدم تناسب الإجراءات في مستوى نظام أسماء النطاقات DNS والأضرار الجانبية). المتطلبات الخاصة بإلزام أمين السجل بتوفير هذه المعلومات سوف تظل سارية في الحالات التي يختار فيها أمين السجل تفويض التحري عن بلاغ انتهاك نظام أسماء النطاقات DNS إلى موزع فرعي. وفي تلك الحالات، يحتفظ أمين السجل بالتزام إيضاح الامتثال للقسم 3.18 من اتفاقية اعتماد أمناء السجلات[10] by عن طريق شرح الإجراءات التي اتخذها إضافة إلى الإجراءات التي اتخذها أي من الأطراف المفوضة الأخرى مثل الموزعين مع توفير السجلات ذات الصلة.

يجري تطبيق سياسات ICANN والمتطلبات التعاقدية ضمن حدود القوانين والأنظمة السارية على كل أمناء السجلات ومشغلي السجلات. ولتجنب حدوث أي شك، لن يكون أمناء السجلات أو مشغلو السجلات مطالبون أو ينتظر منهم اتخاذ أي إجراء يتعارض مع القوانين والأنظمة المرعية.

تتوفر معلومات حول موعد وكيفية ومكان تقديم الشكاوى إلى إدارة الامتثال التعاقدي في ICANN هنا.

[10] انظر القسم 3.12 من اتفاقية اعتماد أمناء السجلات.