ضمانات برنامج gTLD الجديد ضد إساءة استخدام نظام أسم النطاق DNS

عمليات ICANN وأبحاث السياسات | مارس 2016

ICANN

جدول المحتويات

مقدمة **1**

إساءة استخدام DNS: المصطلحات الرئيسية **3**

مجموعة عمل سياسات إساءة التسجيل 4

إساءة استخدام DNS: الإحصاءات والاتجاهات الرئيسية **8**

إساءة استخدام DNS في نطاقات gTLD الجديدة **10**

دراسة حالة لإساءة استخدام DNS: التصيد في نطاقات gTLD الجديدة 11

الضمانات التسع **12**

سؤال: كيف نضمن عدم إدارة أشخاص سيئين للسجلات؟ **12**

الضمانة: تدقيق مشغلي السجل 13

سؤال: كيف نضمن صحة واستخدام معلومات السجل؟ **14**

الضمانة: طلب خطة موضحة لنشر DNSSEC 14

الضمانة: حظر البدل 16

الضمانة: استبعاد السجلات المتبقية الوحيدة 17

سؤال: كيف نضمن تركيز الجهود أكثر على مكافحة المخالفات المحددة؟ **18**

الضمانة: مطلب لسجلات WHOIS المفصلة 18

الضمانة: مركزية الوصول إلى ملف المنطقة 20

الضمانة: توثيق اتصالات وإجراءات إساءة الاستخدام على مستوى السجل 21

الضمانة: المشاركة في عملية طلب أمان السجل المرسل (ERSR) 22

سؤال: كيف نقدم إطار مراقبة محسن لنطاقات TLD مع احتمالية فعلية لوجود سلوك ضار؟ **22**

الضمانة: إنشاء مسودة إطار لبرنامج لتحقق من المنطقة عالية الأمان 22

العروض والنماذج البحثية **24**

إطار كمي محتمل لاختبار فاعلية الضمانات **24**

تصميم البحث: الأسئلة والاعتبارات الرئيسية 25

النماذج والافتراضات العابرة 26

الملحق: استبيان الأنشطة المرتبطة بإساءة الاستخدام في ICANN **28**

مقدمة

وفقًا للبند 9.3 من تأكيد الالتزامات في ICANN الذي ينص على دعم المنافسة واختيار المستهلك وثقة المستهلك في نظام اسم النطاق، يقصد من هذا التقرير دعم أعمال فريق المراجعة حول المنافسة واختيار المستهلك وثقة المستهلك. وسيقوم بذلك من خلال ما يلي:

- تقديم نظرة عامة على حالة انتهاكات نظام اسم النطاق عقب طرح برنامج نطاقات المستوى الأعلى العامة (gTLD) في يناير 2012
- مناقشة خيارات قياس فاعلية ضمانات تفعيل الضمانات التسع لتلافي انتهاكات DNS في نطاقات gTLD الجديدة
- اقتراح نموذج بحثي للمساعدة في تقييم فاعلية الضمانات التسع في تلافي انتهاكات DNS في نطاقات gTLD الجديدة

ينص تأكيد الالتزامات على ما يلي:

> سوف تنظم ICANN مراجعة لدراسة مدى تشجيع التوسع في نطاقات gTLD للمنافسة وثقة المستهلك واختيار المستهلك، فضلاً عن فعالية ...الضمانات التسع المفعلة للتخفيف من القضايا التي تنطوي عليها عملية ...التوسع... [تمت إضافة التأكيد]. سيتم تنفيذ المراجعة من خلال أعضاء متطوعين من المجتمع مع تعيين فريق المراجعة ونشره للتعليق العام... كما سيتم توفير التوصيات الناتجة من المراجعات إلى مجلس الإدارة وإرسالها للتعليق العام. وسيتخذ مجلس الإدارة إجراءات خلال فترة ستة شهور من استلام التوصيات

عند الإعداد للتوسع المحتمل لنظام اسم النطاق، طلبت ICANN النصيحة من دوائرها الخبيرة للتحقق من احتمالية زيادة الأنشطة المخالفة والضارة والإجرامية في نظام اسم النطاق الموسع وتقديم التوصيات للتخفيف الاستباقي من هذه الأنشطة من خلال عدد من الضمانات التسع.[1] وقد بدأت جهود تحديد الخطوات للتخفيف من الانتهاكات المحتملة بطرح أربعة أسئلة على الخبراء في مجموعات متنوعة بما في ذلك مجموعة عمل مكافحة التصيّد (APWG)، فريق تسجيل السلامة على الإنترنت (RISG)، اللجنة الاستشارية للأمن والاستقرار (SSAC)، فرق الاستجابة للطوارئ (CERTs)، دائرة الملكية الفكرية (IPC)، وأعضاء المجتمعات المصرفية والمالية وأمن الإنترنت. وفيما يلي هذه الأسئلة:

1) كيف نضمن عدم إدارة أشخاص سيئين للسجلات؟
2) كيف نضمن صحة واستخدام معلومات السجل؟
3) كيف نضمن تركيز الجهود أكثر على مكافحة المخالفات المحددة؟
4) كيف نقدم إطار مراقبة محسن لنطاقات TLD مع احتمالية فعلية لوجود سلوك ضار؟

---

[1] "التخفيف من السلوك الضار"، ICANN، تفسير برنامج gTLD الجديد مذكرة بتاريخ 3 أكتوبر 2009، https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf

بعد المشاورات الموسعة، توصلت مجموعات الخبراء إلى التوصيات التالية لتناول كل مجال مشكلات:

السؤال	التوصية (التوصيات)
1) كيف نضمن عدم إدارة أشخاص سيئين للسجلات؟	1) فحص مشغلي السجلات من خلال فحوصات البيانات الأساسية للحد من مخاطر مشاركة أحد مشغلي السجلات المحتملين في سلوك إجرامي أو ضار أو بسوء نية.
2) كيف نضمن صحة واستخدام معلومات السجل؟	2) طلب نشر الملحق الأمني لنظام اسم النطاق (DNSSEC) في كافة السجلات الجديدة للحد من احتمالية سجلات DNS المخادعة. 3) حظر "البدل" لمنع إعادة توجيه DNS والردود المركبة لنظام DNS التي قد يترتب عليها الوصول إلى المواقع الضارة. 4) تشجيع استبعاد السجلات المجمعة الفردية للحد من استخدام بقايا النطاقات المستبعدة سابقًا من السجلات كملاذ آمن لإدخالات خادم الاسم في ملف منطقة TLD الذي يمكن للمستخدمين السيئين استخدامه.
3) كيف نضمن تركيز الجهود أكثر على مكافحة المخالفات المحددة؟	5) مطالبة سجلات WHOIS القوية بتشجيع توفر واكتمال البيانات. 6) مركزية الوصول الى ملف المنطقة لإنشاء وسيلة أكثر كفاءة للحصول على التحديثات حول النطاقات الجديدة بمجرد إنشائها داخل كل منطقة TLD. 7) توثيق المخالفات على مستوى السجل وأمناء السجل للعقود والسياسات لتوفير جهة اتصال واحدة لتناول شكاوى المخالفة. 8) تقديم عملية عاجلة للطلب الأمني للسجل للتعامل مع التهديدات الأمنية التي تتطلب اتخاذ إجراء فوري من السجل ورد عاجل من ICANN.
4) كيف نقدم إطار مراقبة محسن لنطاقات TLD مع احتمالية فعلية لوجود سلوك ضار؟	9) إنشاء مسودة إطار لبرنامج التحقق من المنطقة الأمنية المرتفعة لإنشاء مجموعة من المعايير لتأكيد الثقة في نطاقات TLD ذات المخاطر الأكبر بالاستهداف من قبل المشاركين السيئين، مثل نطاقات TLD للخدمات المصرفية والمستحضرات الدوائية، من خلال الضوابط التشغيلية والأمنية المحسنة.

يعتبر قياس فاعلية الضمانات التسع أحد الأهداف المركزية لأعمال CCT-RT. ولدعم هذه الأعمال، سيعرض التقرير فحصًا متعمقًا لكل من الضمانات التسع بجانب اقتراح الوسائل المحتملة لقياس فاعليتها عند الإمكان ووضع نموذج بحثي لتحليل فاعليتها بصورة قوية وشاملة. لاحظ أن المقصود من هذا التقرير هو مساعدة CCT-RT. كما يقصد أن يعرض الوسائل المحتملة بجانب تحفيز النقاش ضمن الفريق حول أفضل طريقة للتعامل مع دراستها لمخالفات DNS والضمانات التسع المعمول بها للتخفيف منها في سياق برنامج gTLD الجديد.

إساءة استخدام DNS: المصطلحات الرئيسية

تغطي إساءة استخدام DNS مجموعة متنوعة من الأنشطة. وبينما لا يوجد تعريف مقبول عمومًا، فإن التعريفات المتغيرة يمكن أن تتضمن الجرائم الإلكترونية والاختراق والسلوك الضار كما كانت تستخدمه ICANN في الماضي. في هذا الصدد، يصنف الباحثون من جامعة روما والمركز العالمي للأمن الإلكتروني هذه التهديدات لنظام DNS على أنها تأتي ضمن ثلاث فئات: تلف البيانات وحجب الخدمة والخصوصية.[2]

"إساءة استخدام DNS" هو المصطلح المستخدم في هذا التقرير ويشير إلى الأنشطة المخادعة أو المتآمرة أو غير اللازمة عن عمد والتي تستفيد من DNS و/أو الإجراءات المستخدم لتسجيل أسماء النطاقات. وهذا تعريف عملي مستند إلى مراجعة للأنشطة المستعرضة بالفعل في المراجع على أنها ضارة أو مخالفة، ويقصد منه تقديم مخرج لفريق CCT-RT لتنقيح التعريف المقدم من جانبه لإساءة استخدام DNS في أعمالهم. وكما هو موضح أدناه، تأتي بعض الأنشطة ضمن نطاق سوء النية في الممارسات التجارية، إلا أنها ليست بالضرورة غير قانونية، بينما الأخرى ممارسات خادعة صريحة يحتمل أن تكون غير قانونية في معظم الاختصاصات حول العالم. كذلك، ستبقي درجة النشاط المخالف (المبينة أدناه) التي يقع بها ضمن هذا التعريف ويمكن تحليله من جانب الضمانات التسع للتخفيف من مخالفة DNS في برنامج gTLD الجديد متاح نظرها من قبل فريق CCT-RT. ويتمثل الهدف في تقديم هيكل تعريفات عملي لتأطير المناقشات الإضافية حول الأنشطة التي يجب إدراجها في الأعمال.

إساءة استخدام DNS: التكتيكات والأدوات

ينفذ المشاركون السيئون عادةً مخططاتهم من خلال الطرق التالية:[3]

- **النطاقات المعرضة:** النطاقات التي يدخل فيها أحد العناصر الضارة إلى الشبكة المستضيفة لأمين السجل.
- **التسجيلات الضارة:** النطاقات التي تسجلها العناصر الضارة لأغراض المشاركة الصريحة في إساءة استعمال DNS.
- **بائعو النطاقات الفرعية:** خدمة، تكون العديد منها مجانية وتعرض التسجيل بدون هوية من خارج خدمة WHOIS، تتيح للأشخاص إجراء عمليات تسجيل على المستوى الثالث أسفل نطاق المستوى الثاني التي يمتلكه مزود الخدمة. ولا يحتفظ البائعون عادة بأي بيانات للتسجيل أو نقطة الاتصال أكثر من مجرد أسماء حسابات المستخدمين.[4]
- **عنوان بروتوكول الإنترنت:** تستخدم هجمات التصيد في بعض الأحيان عناوين بروتوكول الإنترنت في عناوين محدد مواقع المعلومات وليس أسماء النطاقات.

---

[2] "Casalicchio, Caselli, and Coletta, "Measuring the Global Domain Name System, IEEE Network 27, no. 1, (2013) 25-31. doi: 10.1109/MNET.2013.6423188

[3] لاحظ أن أول عنصرين مدرجين هما الطريقتان الرئيسيتان المستخدمة من قبل المشاركين السيئين. راجع Illumintel، "احتمالية تصيد نطاقات المستوى الأعلى للسلسلة الحساسة"، دراسة لجنة برنامج gTLD الجديد لمجلس إدارة ICANN https://www.icann.org/resources/pages/new-gtld-program-committee-2014-03-21-en

[4] Anti-Phishing Working Group, "Making Waves in the Phisher's Safest Harbor: Exposing the Dark Side of Subdomain Registries," November 2008, http://docs.apwg.org/reports/APWG_Advisory_on_Subdomain_Registries.pdf

- **عناوين محدد مواقع المعلومات المختصرة:** أسلوب لضغط عناوين النطاق الطويلة التي يمكن أن يستخدمها العناصر الضارة للتشويش على اسم النطاق وبالتالي إعادة توجيه المستخدمين المطمئنين إلى المواقع الضارة[5]

يمكن أن تأخذ إساءة استعمال DNS عددًا من الأشكال إلا أن الهدف النموذجي لها هو مقاطعة البرامج الضارة المستخدمة لتعطيل عمليات الكمبيوتر، أو تجميع المعلومات الحساسة أو الوصول إلى أنظمة الكمبيوتر الخاصة.[6] كما يمكن أن تنفذ البرامج الضارة نفسها عددًا من الأنشطة الضارة والتي تأخذ عددًا من الأشكال. تشمل أشهر البرامج الموزعة ما يلي:

- **الفيروسات:** البرامج الضارة التي تنفذ عددًا من الأنشطة غير المرغوبة والتسبب في عدم عمل أجهزة الكمبيوتر بصورة مناسبة، بما في ذلك إنشاء ونقل ومسح الملفات، و/أو استهلاك ذاكرة الكمبيوتر. كذلك، تقوم الفيروسات عادة بتكرار نفسها والانتقال عبر الشبكات من خلال عناوين البريد الإلكتروني المصابة. وتتضمن الأمثلة الفيروسات المتنقلة وأحصنة طروادة.[7]
- **برامج التجسس:** البرامج الضارة التي يمكن أن تستحوذ على المعلومات مثل أسماء المستخدمين وكلمات المرور ومعلومات بطاقة الائتمان وعادات استعراض الويب وعناوين البريد الإلكتروني.[8]

إضافة إلى ذلك، تنتشر البرامج الضارة عادة عبر استخدام برامج التتبع، وهي برامج تلقائية مشفرة للعمل باستمرار على تنفيذ الوظائف الضارة أو المخالفة.[9] شبكات Botnet هي شبكات برامج التتبع التي تستخدم أجهزة الكمبيوتر المصابة لنشر البرامج الضارة.[10] ولا يعرف الأشخاص الذين تتعرض أجهزتهم للإصابة أنها تستخدم لهذا الغرض.

مجموعة عمل سياسات إساءة التسجيل

في 2010، أصدرت مجموعة عمل سياسات إساءة التسجيل في GNSO تقريراً حول إساءة استخدام التسجيل في اتفاقيات السجلات - المسجلين. وفي هذا التقرير، وضعت المجموعة تعريفًا بالإجماع لإساءة الاستخدام ونصه كما يلي:

> إساءة الاستخدام هو إجراء: أ) يتسبب في ضرر فعلي وموضوعي أو توقع ماضي بالضرر، ب) إجراء غير قانوني أو غير شرعي أو يعتبر مخالفًا للهدف والتصميم ذي الغرض الشرعي المعلن عنه، إذا تم الإعلان عن هذا الهدف.[11]

---

[5] راجع StopTheHacker.com, "The Curse of the URL Shorteners: How Safe Are They?" بتاريخ 26 فبراير 2016، https://www.stopthehacker.com/2010/02/19/analyzing-url-shorteners/

[6] مجموعة التنفيذ الاستشارية المختصة بالتنافس وثقة المستهلك واختيار المستهلك (IAG-CCT): التوصيات النهائية حول مقاييس مراجعة CCT، 26 سبتمبر 2014، https://newgtlds.icann.org/en/reviews/cct/iag-metrics-final-recs-26sep14-en.pdf

[7] Kaspersky Lab, "What is a Computer Virus or a Computer Worm?" بتاريخ 26 فبراير 2016، http://www.kaspersky.com/internet-security-center/threats/viruses-worms

[8] Kaspersky Lab, "What is Spyware?" بتاريخ 26 فبراير 2016، http://usa.kaspersky.com/internet-security-center/threats/spyware#.VtCsAJMrJTY

[9] لا تكون برامج التتبع عادةً ضارة وتنفيذ أي عدد من الوظائف المسموح بها. ومع ذلك، لا يتعامل هذا التقرير سوى مع شكلها الضار. راجع Gabada, Usman, and Sharma, "Techniques to Break the Botnet Attack," International Journal for Research in Emerging Science and Technology 2، رقم 1 (مارس 2015)، http://ijrest.net/downloads/volume-2/special-issue-1/pid-m15ug638.pdf

[10] المصدر ذاته.

[11] "التقرير النهائي لمجموعة عمل سياسات إساءة استخدام التسجيل"، مايو 2010 http://gnso.icann.org/en/issues/rap/rap-wg-final-report-29may10-en.pdf

من ناحية أخرى، فقد تعرضوا بصورة أكبر للتمييز بين إساءة الاستخدام والتسجيل، مع إشارة الأولى إلى المشكلات التي تنشأ أثناء تسجيل النطاقات، بينما تشير الثانية إلى كيفية استخدام النطاقات بعد التسجيل. ويتضمن إطار التعريف ما يلي:

مشكلات التسجيل تعتبر ذات صلة بالأنشطة المتصلة باسم النطاق الأساسية التي يتم تنفيذها من مسجلين وسجلات. وهي تتضمن عموما (مع عدم حصرها على ذلك) تحديد الأسماء المسجلة والصيانة والوصول إلى معلومات التسجيل (WHOIS) وحالات نقل وحذف وإعادة تحديد أسماء النطاق والنقاط الأخرى المشابهة التي تمت مناقشتها بمزيد من التفصيل أدناه. وهي عموما ضمن نطاق سلطة GNSO. وقد تم إدراج العديد من هذه الأشياء بشكل خاص في اتفاقيات التسجيل كما أنها تخضع للسياسات التوافقية والمزيد من السياسات التوافقية التي يتوجب تنفيذها فيما يخص هذه الأنواع من الموضوعات.

كذلك، ناقشت المجموعة الأنشطة التالية كأشكال محتملة لإساءة استخدام التسجيل:

- **الاحتلال الإلكتروني** - التسجيل والاستخدام المتعمد بسوء نية لاسم يمثل علامة مسجلة أو علامة لجهة غير مرتبطة، عادة لأغراض تحقيق الربح (عادة، بالرغم من أنه غير حصري، فمن خلال إعلانات الدفع مقابل كل نقرة).
- **المعلومات المسبقة** - عندما يحصل أحد الأطراف على شكل ما من المعلومات الداخلية فيما يتعلق بتفضيل مستخدم الإنترنت لتسجيل اسم النطاق واستخدام هذه الفرصة للتسجيل الاستباقي لاسم النطاق.
- **المواقع المشتكية** - مواقع الويب التي تشتكي من منتجات أو خدمات أحد الشركات أو الجهات وتستخدم العلامة التجارية للشركة في اسم النطاق (مثل companysucks.example). كذلك، كانت المخاوف التي عبرت عنها المجموعة من أن أنواع المواقع هذه يمكن أن تنتهك حقوق مالكي العلامات التجارية. إلا أن المجموعة لاحظت أيضًا أنه في العديد من الحالات تكون هذه المواقع طرق للشكاوى الشرعية وتتم حمايتها بموجب قوانين حرية التعبير في العديد من الاختصاصات.
- **أسماء النطاق المخادعة و/أو المنتهكة** - تسجيل أسماء النطاقات التي توجه المستخدمين المطمئنين إلى المواقع الفاضحة أو القصر إلى المحتوى الضار، وفي بعض الأحيان يشار إليها كأحد أشكال "التحريض بالخداع".
- **ملاحظات التجديد المزيفة** - مراسلات مضللة مرسلة إلى أمناء السجل من أحد الأفراد أو المؤسسات تطالبه بالتسجيل أو تمثيل المشترك الحالي. وترسل هذه الرسائل للعديد من الأغراض المخادعة.
- **صياغة الاسم** - استخدام أدوات تلقائية لإنشاء تباديل لسلسلة اسم نطاق محددة. وبينما يستخدم المشتركون عادةً هذه الأدوات بصورة شرعية لاقتراح أسماء بديلة للمشتركين المحتملين عندما لا يتوفر اسم السلسلة الذي يرغب فيه المشترك، فقد كانت مخاوف المجموعة من أن هذه الأدوات يمكن أن تتسبب في مخالفات لسلاسل العلامات التجارية.
- **الدفع لكل نقرة** - نموذج إعلان عبر الإنترنت يستخدم في مواقع الويب ويدفع فيه المعلن للمضيف فقط عند النقر على الإعلان. في هذا الصدد، كانت المخاوف المطروحة تتعلق باستخدام علامة تجارية في أحد أسماء النطاقات لجذب الحركة إلى أحد المواقع التي تتضمن إعلانات مدفوعة.
- **تحويل الحركة** - استخدام أسماء النطاقات في صورة نص HTML مرئي، أو نص مخفي أو علامات بيانات أو عنوان صفحة ويب للتلاعب بتصنيفات محرك البحث وتوجيه الحركة.
- **التبعية الزائفة** - الادعاء زيفًا بالتبعية لمالك علامة تجارية.
- **الممارسات الخادعة للتسجيل عبر نطاقات TLD** - ممارسات بيع مخادعة يرسل فيها إخطار لأحد المشتركين بأن هناك طرف آخر مهتم أو يحاول تسجيل سلسلة نطاق المشترك في TLD آخر. ولذلك، يطلب من المشترك تنفيذ عمليات تسجيل إضافية من خلال الطرف المرسل للإخطار، عادة ما يكون بائع سيربح من عمليات التسجيل الإضافية ويعرض النطاق الجديد المنشأ بسعر سوقي أعلى من المتوسط.
- **التسجيل المكرر للنطاق** - عندما يسيء المشتركون استخدام فترة السماح الإضافية عبر التسجيل المستمر أو الحذف أو إعادة تسجيل نفس أسماء لتجنب دفع رسوم التسجيل.

على النقيض عرفت RAPWG "الاستخدام" كما يلي:

> إن مشكلات استخدام اسم النطاق ترتبط بما يفعله المسجل باسم النطاق لديه بعد إنشاء هذا النطاق - والهدف الذي من أجله تم وضع النطاق من المسجل و/أو الخدمات التي يعمل عليها المسجل. وتكون مشكلات الاستخدام المذكورة عادةً مستقلة أو لا تتضمن أي مشكلات تسجيل... استخدام اسم النطاق في منطقة تكون فيها سلطة ICANN وسلطة اتخاذ قرار من GNSO محدودة أكثر.

كذلك، ناقشت المجموعة الأنشطة التالية كأشكال محتملة لإساءة الاستخدام:

- **التصيد** - موقع ويب يعرض نفسه بصورة محتالة كموقع موثوق به (عادة بنك) لخداع مستخدمي الإنترنت للكشف عن معلومات حساسة (مثل بيانات الاعتماد البنكية على الإنترنت وكلمات مرور البريد الإلكتروني). ويتمثل الهدف من التصيد عادةً في سرقة الأموال أو الأصول القيمة الأخرى.
- **البريد غير المرغوب فيه** - بريد غير مرغوب فيه مرسل من نطاقات ويستخدم للإعلان عن مواقع الويب.
- **التحكم والسيطرة لشبكات بوتنت/البرامج الضارة** - استخدام أسماء النطاقات كطريقة للتحكم في شبكات بوتنت وتحديثها، وهي شبكات تتضمن آلاف أو حتى ملايين أجهزة الكمبيوتر المصابة تحت السيطرة المشتركة لأحد العناصر الإجرامية. ويمكن استخدام شبكات بوتنت عادةً لارتكاب العديد من الأنشطة الضارة، بما في ذلك هجمات حجب الخدمة الموزعة والبريد غير المرغوب به والتمويه السريع والتصيد والمواقع غير المرغوب بها (تجد أدناه مزيد من التوضيح حول الممارسات والمصطلحات المستخدمة في هذا التعريف).
- **استخدام بيانات اعتماد مسروقة** - مثل الهوية والوصول والبيانات المالية لتسجيل أسماء النطاقات لأغراض ضارة والسرقة من أو المقاطعة بخلاف ذلك لعمليات الأفراد أو المؤسسات.

وفي التقرير، أكدت RAPWG على أن ICANN لديها في العديد من المنظمات الداعمة اختصاص فيما يتعلق بمشكلات التسجيل من خلال عمليات صنع السياسات والتنفيذ، بينما تكون مشكلات الاستخدام أكثر صعوبة في مواجهة صلاحيات ICANN المحدودة فيما يتعلق بكيفية استخدام المشتركين لأسماء النطاقات. لاحظ أن التعريفات والأنشطة التي يتناولها هذا القسم كانت تلك التي ناقشها أعضاء RAPWG لأغراض التقرير ولا تشكل اعتمادًا من ICANN فيما يتعلق بالأنشطة التي تشكل في الواقع إساءة استخدام DNS. وتعمل التعريفات والأنشطة المذكورة هنا على خدمة أعمال CCT-RT، كما أنها لأغراض العلم والمناقشة فقط.

المادة 11 من اتفاقية سجل gTLD الجديد

تنص المادة 11 من اتفاقية سجل gTLD الجديد على التزام مشغلي السجلات ببعض التزامات المصلحة العامة كجزء من التزاماتهم التعاقدية مع ICANN. ويركز البندان الفرعيان 3أ و3ب على التزامات المصلحة العامة لمشغلي السجلات كجانب من إساءة استخدام DNS، وتبين الأنشطة التي يجب إدراجها في جهودهم للتخفيف من السلوك المخالف في نطاقات TLD وتتبعه. تنص المادة رقم 11 على الآتي:[12]

> 3أ. يلتزم مشغل السجل بإدراج حكم في اتفاقية السجل-أمين السجل تشترط على أمناء السجلات إدراج أحكام اتفاقيات التسجيل الخاصة بهم تحظر على حاملي اسم المسجل من توزيع البرامج الضارة أو شبكات بوتنت التشغيلية الضارة أو رسائل التصيد أو القرصنة أو العلامات التجارية أو التعدي على حقوق المؤلف أو الممارسات الاحتيالية أو المضللة أو التزوير أو الانخراط في أنشطة خلاف ذلك تتعارض مع القوانين المعمول بها وتزويد (بما يتفق مع القوانين المعمول بها وأي إجراءات ذات صلة) عواقب لمثل هذه الأنشطة بما في ذلك تعليق اسم المجال.
>
> 3ب. يلتزم مشغل السجل بإجراء تحليل فني دوري لتقييم ما إذا كانت النطاقات في نطاق TLD الخاص به يجري استخدامه في ارتكاب تهديدات للأمن أم لا، مثل السطو على مواقع الويب، والاحتيال، والبرامج

[12] "اتفاقية السجل" بتاريخ 4 فبراير 2016، https://www.icann.org/resources/pages/registries/registries-agreements-en

الضارة، وشبكات بوتنت. كما يلتزم مشغل السجل بالحفاظ على تقارير إحصائية حول عدد تهديدات الأمان المحددة والإجراءات التي يتم اتخاذها نتيجة لفحوصات الأمن الدورية. ويلتزم مشغل السجل بالحفاظ على هذه التقارير طوال مدة هذه الاتفاقية ما لم يقتضي القانون فترة أقصر أو الموافقة عليها من جانب ICANN، وتقديمها إلى ICANN لدى طلبها.

كذلك، قد تقدم الأنشطة المبينة ضمن المادة 11 إطار تعريف إضافي لمجموعة CCT-RT عند تعديل نطاق المراجعة.

إساءة استخدام DNS: المصطلحات والاعتبارات الإضافية

يجدر ذكر عددًا من المصطلحات والاعتبارات الأخرى فيما يتعلق بالأنشطة التي تشكل إساءة استخدام DNS:

- يستخدم التصيد كلاً من الهندسة الاجتماعية والخدع الفنية؛ للاستيلاء على بيانات الهوية الشخصية وبيانات اعتماد الحسابات المالية للعملاء. وتستخدم أساليب الهندسة الاجتماعية رسائل بريد إلكتروني مخادعة لتوجيه العملاء لمواقع ويب زائفة، مصممة لمخادعة المستلمين، ليقوموا بإفشاء البيانات المالية الخاصة بهم مثل: أرقام بطاقات الائتمان واسم مستخدم الحساب وكلمة المرور وأرقام الضمان الاجتماعي. التصيد الموجه - نوع محدد من البريد غير المرغوب فيه للتصيد يستهدف أفراد محددين ببيانات اعتماد متميزة لدى أحد المؤسسات بهدف خداعهم لتقديم معلومات حساسة.[13]
- التمويه السريع هو أسلوب تنفذه شبكات بوتنت في التصيد والبريد غير المرغوب فيه وأنشطة تقديم البرامج الضارة الأخرى ترسل فيه الهجمات من مجموعة تتحول باستمرار لعناوين IP مما يزيد من صعوبة اكتشافها.[14]
- الاختراق بالطباعة - يعرف أيضًا بسرقة URL، هو أحد أشكال الاختراق الإلكتروني الذي يعتمد على المستخدمين الذين يخطؤون في الكتابة عند إدخال عنوان موقع ويب في المستعرض وعادة يوجه المستخدمين إلى مواقع ضارة.[15]
- الإعلانات الخبيثة هي إعلانات على مواقع الويب أو شبكة إعلانات يتم إعدادها لإصابة من يعرضها ببرامج ضارة سواء كل مرة يراها فيها أو على فترات متعددة حسب الوقت وعدد مرات الضغط.[16]
- اختراق محرك البحث هو نشاط يتلاعب بمحركات البث لعرض نتائج بحث تتضمن روابط إلى مواقع الويب الضارة.[17]
- تحدث الهجمات المخادعة عندما ينتحل عنصر ضار صفة جهاز أو مستخدم آخر لبدء هجمات ضد مستضيفي الشبكة أو سرقة البيانات أو نشر البرامج الضارة أو تجاوز عناصر التحكم الأمنية.[18]
- هجمات حجب الخدمة الموزعة هي هجمات إلكترونية تعمل على عدم توفير واحد أو أكثر من أنظمة الكمبيوتر. وتحدث الهجمة الموزعة، تنفذ عبر شبكة بوتنت، عندما تنسق أنظمة متعددة للتغلب على خوادم الضحايا بالطلبات. كما ظهر شكل جديد من هجمات DDoS المضخمة والذي يستخدم انعكاس DNS

---

[13] استشارة SSAC حول حماية المسجل: أفضل الممارسات من أجل الحفاظ على الأمن والاستقرار في دورة حياة إدارة الاعتمادات، اللجنة الاستشارية للأمن والاستقرار في ICANN، نوفمبر 2015، https://www.icann.org/en/system/files/files/sac-074-en.pdf

[14] "استشارة SSAC حول استضافة التمويه السريع ونظام DNS"، اللجنة الاستشارية للأمن والاستقرار في ICANN، مارس 2008 https://www.icann.org/en/system/files/files/sac-025-en.pdf

[15] Moore and Edelman، "قياس مرتكبي وممولي الاختراق بالطباعة"، العاملين بهذا الحقل والمؤسسين لحالا الاستيلاء" الورقة المقدمة في المؤتمر الدولي للاستيلاء للأغراض المالية وأمن البيانات، تينيريفي، يناير 2010 http://www.benedelman.org/typosquatting/typosquatting.pdf

[16] تقرير اجتماع الندوة الرابعة حول مرونة واستقرار وشفافية نظام أسماء النطاقات العامة، https://www.icann.org/en/system/files/files/dns-symposium-25oct12-en.pdf

[17] "اختراق محركات البحث"، Imperva، بتاريخ 1 فبراير 2016 https://www.imperva.com/resources/glossary?term=search_engine_poisoning_sep

[18] Veracode، "الهجمات المخادعة: IP وDNS وARP"، بتاريخ 4 فبراير 2016 http://www.veracode.com/security/spoofing-attack

وتضخيمه لتحقيق معدلات بت مرتفعة للغاية للهجمات (تتجاوز عادةً 300 جيجابايت لكل ثانية)، والتي تزيد عن سعة شبكة الضحية مما يترتب عليه انقطاع كبير أو كامل للخدمة.[19]

- تظليل النطاق هو أحد الأشكال الأخرى لإساءة استعمال DNS حيث تستخدم العناصر الإجرامية بيانات اعتماد مسروقة أو مخترقة لإنشاء العديد من النطاقات الفعلية المرتبطة بنطاقات صحيحة قائمة في مجموعة المشترك. وتستمر النطاقات الصحيحة في العمل بصورة عادة من وجهة نظر المشترك إلا أن هذه النطاقات الفرعية توجه الزوار إلى مواقع ضارة.[20]
- اختراق ذاكرة DNS المؤقتة هي هجمة يخدع فيها عنصر ضار خادم الاسم من خلال إضافة أو تعديل بيانات DNS المخزنة ببيانات ضارة. الخداع هو أحد أشكال هذا النشاط حيث يخادع أحد العناصر الضارة الضحية للنقر فوق رابط، يرسل عادة عبر البريد غير المرغوب فيه، والذي يصيب بدوره الكمبيوتر الشخصي للضحية أو الخادم ويعيد توجيه المستخدمين إلى المواقع المحتالة حيث يمكن تجميع المعلومات الشخصية السرية.[21]

أحد العوامل الرئيسية اللازم تذكرها عندما يتعلق الأمر تقريبًا بكافة هذه الأساليب هو أنها تستخدم نقاط الضعف البشرية في صورة الطمع أو الإهمال أو السذاجة. وبهذا، يمكن أن يشكل المستخدمون النهائيون الرابط الأضعف في سلسلة الأمن الإلكتروني.[22]

إساءة استخدام DNS: الإحصاءات والاتجاهات الرئيسية

أظهر استطلاع عالمي حديث تحت رعاية ICANN لعدد 6144 من العملاء ما يلي:

- 74% يعلمون ما هو التصيد
- 79% يعلمون ما هو البريد غير المرغوب فيه
- 40% يعلمون ما هو الاختراق الإلكتروني
- 67% يعلمون ما هي بيانات الاعتماد المسروقة
- 76% يعلمون ما هي البرامج الضارة

بجانب المعرفة الكبيرة بالسلوك الضار في DNS، أوضح المستخدمون النهائيون أيضًا مستويات عالية من الخوف الكبير من كل سلوك مخالف، بجانب اعتقادهم بأنها أيضًا شائعة للغاية/إلى حد ما.[23]

---

[19] "استشارة SSAC حول هجمات DDoS لدعم بنية DNS الأساسية"، اللجنة الاستشارية للأمن والاستقرار في ICANN، مارس 2014 https://www.icann.org/en/system/files/files/sac-065-en.pdf.
راجع أيضًا Alvarez, Carlos, "Amplified DDoS Attacks: The Current Biggest Threat Against the Internet"، مدونة 11، ICANN أبريل 2014،
https://www.icann.org/news/blog/amplified-ddos-attacks-the-current-biggest-threat-against-the-internet

[20] استشارة SSAC حول حماية المسجل: أفضل الممارسات من أجل الحفاظ على الأمن والاستقرار في دورة حياة إدارة الاعتمادات، اللجنة الاستشارية للأمن والاستقرار في ICANN، نوفمبر 2015،
https://www.icann.org/en/system/files/files/sac-074-en.pdf

[21] راجع Piscitello, Dave, "DNS Pharming: Someone's poisoned the water hole!" WatchGuard Technologies Expert Editorial, 2005,
http://www.corecom.com/external/livesecurity/dnsphishing.htm

[22] Khonji, Mahmoud and Youssef Iraqi, "Phishing Detection: A Literature Survey" IEEE Communications Surveys & Tutorials 15, no. 4 (Q4 2013), .doi: 10.1109/SURV.2013.032213.00009

[23] أبحاث المستهلك العالمية من ICANN، أجراها نيلسن، أبريل 2015،
https://www.icann.org/news/announcement-2015-05-29-en

أصدرت Symantec، أحد أكبر شركات الأمن الإلكتروني في العالم، تقريرًا سنويًا حول حالة أمن الإنترنت العالمي.[24] وتقدم آخر التقارير عددًا من المؤشرات لتوضيح الاتجاهات العامة في الأنشطة الرئيسية المرتبطة بإساءة استخدام DNS. وبهذا، يمكن أن تعمل فقط كنقطة خروج لتحليل أكثر تقسيمًا لإساءة استخدام DNS في نطاقات gTLD الجديدة والقديمة كأحد الأعمال التي تتقدم فيها CCT-RT:

المؤشر	إحصائيات توضيحية	الاتجاه
مواقع الويب التي وجد بها برامج ضارة	• 2014: 1 في 1126 • 2013: 1 في 566	↓
معدل البريد غير المرغوب فيه الكلي (نسبة كافة رسائل البريد المصنفة كبريد غير مرغوب فيه)	• 2015: 54%[25] • 2014: 60% • 2013: 66%	↓
حجم البريد غير المرغوب فيه العالمي لكل يوم (مقدر)	• 2014: 28 بليون • 2013: 29 بليون	↓
معدل تصيد البريد الإلكتروني (نسبة رسائل البريد الإلكتروني التي تمثل محاولات للتصيد)	• 2014: 1 في 965 • 2013: 1 في 392	↓
متغيرات البرامج الضارة الجديدة المضافة كل سنة	• 2014: 317 مليون • 2013: 252 مليون	↑
معدل البرامج الضارة في البريد الإلكتروني (نسبة رسائل البريد الإلكتروني التي تتضمن برامج ضارة)	• 2014: 1 في 244 • 2013: 1 في 196 • 2012: 1 في 291	↓
عدد برامج التتبع	• 2014: 1.9 مليون • 2013: 2.3 مليون • 2012: 3.4 مليون	↓

بينما توضح هذه البيانات عامةً انخفاض التوجه في الأشكال المحددة لإساءة استخدام DNS، جدير بالذكر أنها تمثل فقط أحد مشاهد هذه الاتجاهات. على سبيل المثال، بينما يبدو أن هجمات التصيد تنخفض وفقًا للجدول، فمند عام 2008، تضاعف تقريبًا عدد هجمات التصيّد، مما يوضح أن الاتجاه المنخفض قد لا يتجاوز مجرد انخفاض بسيط

---

[24] Symantec, "Internet Security Threat Report 20," أبريل 2015، https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf

[25] يمكنك الاطلاع هذا الرقم لسنة 2015 مأخوذ من تقرير معلومات Symantec لشهر نوفمبر 2015 على www.symantec.com/content/en/us/enterprise/other_resources/intelligence-report-11-2015-en-us.pdf. الرقم المدرج هو رقم سنوي ناقصًا تقارير شهر ديسمبر 2015. لم تقدم Symantec تقارير أرقام 2015 السنوية للمقاييس الأخرى المدرجة في هذا الجدول.

في خط التوجه الكلي.[26] علاوة على ذلك، تغطي البيانات المعروضة كامل DNS، إلا أنها لا تبين بالتحديد سوء استخدام DNS في نطاقات gTLD الجديدة

إساءة استخدام DNS في نطاقات gTLD الجديدة

تم إجراء بضعة دراسات منتظمة حول إساءة استخدام DNS في نطاقات gTLD الجديدة والتي تمثل وظيفة محتملة لحداثتها. كما أظهر الاستبيان الممول من ICANN المشار إليه أعلاه أن ثقة المستهلك في نطاقات gTLD الجديدة أقل بكثير من نطاقات TLD القديمة، مع إبداء حوالي 50% من المستهلكين لثقتهم في الجديد مقابل تقريبًا 90% واثقين في نطاقات TLD القديمة.[27] كما توصلت الأبحاث من جامعة كاليفورنيا، سان دييجو إلى أن نطاقات TLD الجديدة أكثر بالضعف على الأرجح من نطاقات TLD القديمة فيما يتعلق بالظهور على قوائم الحظر للنطاقات، قائمة نطاقات البريد غير المرغوب فيه المعروفة، خلال أول شهر من التسجيل.[28]

وفقًا لأعضاء APWG، يبدو أن العناصر الضارة تختبر مساحة gTLD الجديد كقاعدة محتملة للأنشطة.[29] فهي تقترح أن هذا قد يكون ناتجًا عن زيادة المنافسة في سوق gTLD الجديدة، والتي تعمل على خفض الأسعار مما يتسبب بدوره في جذب العناصر الضارة للنظر في الرسملة بتكاليف أقل. ومع ذلك، يلاحظ الأعضاء صعوبة في التوصل إلى نتائج وفقًا للدليل المقارن المحدود المقدم بأن نطاقات gTLD الجديدة في مراحل مبكرة من طرحها. فهي تقترح أن الدراسات المستقبلية تقارن إساءة استعمال DNS في نطاقات TLD الجديدة والقديمة عند توفر ما يكفي من البيانات.[30]

تعرض Architelos، شركة الاستشارات والإدارة لنطاق TLD، تحليل أكثر تفصيلاً لإساءة استخدام DNS في نطاقات TLD الجديدة والقديمة والخاصة برموز الدول (نطاقات ccTLD). كما يستخدم أحدث التقارير، الصادر في يونيو 2015، مؤشر جودة مساحة الاسم والذي يمثل مقدار نطاقات إساءة الاستخدام المدرجة في قائمة الحظر لكل مليون نطاق قيد الإدارة في كل سجل، وذلك لتحليل حالة السلوك المخالف في نطاقات gTLD القديمة والجديدة. كما يعرض التقرير عددًا من النتائج المهمة:[31]

- وفقًا لمؤشر جودة مساحة الاسم من يناير 2014 إلى يونيو 2015، فقد شهد معدل الأنشطة المخالفة (التصيد والبرامج الضارة والتحكم والسيطرة في شبكة بوتنت والبريد غير المرغوب فيه) في نطاقات gTLD الجديد ارتفاعًا كبيرًا منذ أول مخالفة تم اكتشافها في نطاقات gTLD الجديدة في فبراير 2014 وهي تقترب من مستويات نطاقات gTLD القديمة.

---

[26] Illumintel, "Potential for Phishing in Sensitive-String Top-Level Domains" دراسة لجنة برنامج gTLD الجديد لمجلس إدارة ICANN
https://www.icann.org/resources/pages/new-gtld-program-committee-2014-03-21-en

[27] أبحاث المستهلك العالمية من ICANN، أجراها نيلسن، أبريل 2015،
https://www.icann.org/news/announcement-2015-05-29-en

[28] لاحظ أن هذا قياس لمشهد مأخوذ في وقت الدراسة ولم يعكس أي تحليل لمدة أطول. راجع Der et al., "From .academy to .zone: An Analysis of the New TLD Land Rush," University of California, San Diego, Department of Computer Science and Engineering, October 2015, doi: 10.1145/2815675.2815696.

[29] مجموعة عمل مكافحة التصيّد، "استبيان التصيد العالمي: الاتجاهات واستخدام اسم النطاق، في النصف الاول من 2014"، 25 سبتمبر 2014، https://apwg.org/apwg-news-center/

[30] المصدر ذاته.

[31] Architelos، "تقرير إساءة الاستخدام من NameSentry℠"، في يونيو 2015،
http://architelos.com/wp-content/uploads/2015/06/Architelos-StateOfAbuseReport2015-webc-FIN.pdf

- تصل رسائل البريد غير المرغوب فيه لنسبة 99% من حالات المخالفة المقررة في نطاقات gTLD الجديدة أثناء الإطار الزمني للتحليل (شكلت رسائل البريد غير المرغوب فيه 90% في نطاقات gTLD القديمة وفي نطاقات ccTLD).
- في مايو 2015، كانت نتائج المؤشر لنطاقات gTLD الجديدة هي 11654 لكل مليون نطاق قيد الإدارة مقارنة بحوالي 16500 لكل مليون في نطاقات gTLD القديمة.
- لا تزال معدلات التصيد والبرامج الضارة والتحكم والسيطرة في شبكة بوتنت في نطاقات gTLD الجديدة منخفضة للغاية مقارنة بنطاقات gTLD القديمة، بالرغم من أن هذا ربما يزداد مع ارتفاع الوعي والاعتماد لنطاقات gTLD الجديدة. كذلك، من مايو 2014 إلى مايو 2015، ارتفع مقدار نطاقات التصيد من سبعة نطاقات محظورة مكتشفة إلى 143، وهي زيادة بعشرين ضعفًا (مقارنة بارتفاع من تقريبًا 7300 إلى 14000 في نطاقات gTLD القديمة لنفس الفترة). ومع ذلك، تركزت نسبة 77% من تقارير التصيد الجديدة بعدد 143 هذه على عشرة من نطاقات gTLD الجديدة فقط.

دراسة حالة لإساءة استخدام DNS: التصيد في نطاقات gTLD الجديدة

يمكن أن يعمل انتشار التصيد كأحد مؤشرات درجة إساءة استخدام العناصر الضارة لنطاقات gTLD الجديدة. وفي دراسة شارك فيها أعضاء APWG، لاحظ الباحثون أن توسع DNS عبر برنامج gTLD الجديد لا يحتمل أن يعمل على زيادة إجمالي عدد حالات التصيد في العالم، إلا أنه سيترتب عليه مواقع جديدة مختلفة يمكن أن تحدث منها هجمات التصيد، حيث تميل عناصر الجرائم الإلكترونية إلى الخروج من TLD إلى آخر مع الوقت.[32] كذلك، لن يسجل المتصيدون عادةً نطاقات لديها أسماء علامات تجارية، بل بدلاً من ذلك، يفضلون سلاسل دون اسم مميز أو وضع اسم علامة تجارية في مكان ما في النطاق الفرعي أو الدليل الفرعي حيث يبحث مالكي العلامات التجارية عادةً عن أسمائهم المستخدمة بصورة غير مناسبة. وفي النصف الثاني من 2014، تضمنت نسبة 1.9% فقط من كافة النطاقات المستخدمة للتصيد اسم علامة تجارية او تعديل لها (عادة تكون بخطأ في التهجئة).

في ورقة تحليلية أخرى كتبها أعضاء APWG، توصل المؤلفون إلى نتيجة مماثلة مع ملاحظة أن نطاقات gTLD الجديدة لم تتسبب في زيادة مفاجأة لحالات التصيد الجديدة. ويستخدم المؤلفون لكلتا الورقتين مقياسًا وهو "نطاقات التصيد لكل 10 آلاف"، والذي يمثل النسبة بين عدد أسماء النطاقات المستخدمة للتصيد في TLD إلى عدد أسماء النطاقات المسجلة في هذا النطاق، كقياس لسلامة نطاقات TLD الجديدة فيما يتعلق بالتصيد.[33] وقد توصل الباحثون في تحليلهم إلى نتيجة بين 3.4 و4.7 من نطاقات التصيد لكل 10 آلاف وهو ما يمثل نتيجة الانتشار المتوسطة للتصيد.[34] ستشير أي نتيجة أعلى من 4.7 إلى أن نطاق TLD فوق مستويات التصيد المتوسطة. وتجدر الإشارة إلى أن متوسط نطاقات التصيد لكل 10 آلاف قد وصل لكافة نطاقات TLD في النصف الثاني من 2014 إلى 3.4. سجلت تسعة نطاقات فقط من بين 295 نطاق gTLD جديد (في 2014) معدل أكبر من 3.4.[35] إضافة إلى ذلك، وصل متوسط وقت التشغيل لهجمات التصيد، أو طول فترة نشاط هذه الهجمات ومقياس رئيسي لقوة جهود المتصيدين، إلى انخفاضات تاريخية، مما يشير إلى بعض النجاح بالنسبة لجهود مكافحة التصيد.[36]

---

[32] Illumintel، "احتمالية تصيد نطاقات المستوى الأعلى للسلسلة الحساسة"، دراسة لجنة برنامج gTLD الجديد لمجلس إدارة ICANN https://www.icann.org/resources/pages/new-gtld-program-committee-2014-03-21-en

[33] مجموعة عمل مكافحة التصيّد، "استبيان التصيد العالمي: الاتجاهات واستخدام اسم النطاق، في النصف الثاني من 2015"، 27 مايو 2015، https://apwg.org/apwg-news-center/

[34] جدير بالذكر أن تقرير APWG من النص الأول لسنة 2014 سجل قياسًا بين 4.1 و4.7. وتتغير هذه القياسات وفقًا لمنحنى نشاط التصيد الكلي.

[35] مجموعة عمل مكافحة التصيّد، "استبيان التصيد العالمي: الاتجاهات واستخدام اسم النطاق، في النصف الثاني من 2015"، 27 مايو 2015، https://apwg.org/apwg-news-center/

[36] كما شهد النصف الثاني من 2014 ارتفاعًا طفيفًا في متوسط أوقات التشغيل من 8 ساعات و42 دقيقة إلى 10 ساعات و6 دقائق. راجع مجموعة عمل مكافحة التصيّد، "استبيان التصيد العالمي: الاتجاهات واستخدام اسم النطاق، في النصف الثاني من 2015"، 27 مايو 2015، https://apwg.org/apwg-news-center/

وفقًا لمؤلفي كلا البحثين، يبدو أن أسعار النطاقات أحد المحركات المهمة للتصيد في نطاقات TLD، حيث تبدو النطاقات أرخص في نطاقات TLD القديمة.[37] وقد ردد هذا الرأي عددًا من الممثلين من السجلات وأمناء السجل في أحد المؤتمرات الهاتفية التي تمولها ICANN عند قياس إساءة استعمال DNS، وهو ما أشار إلى أن ارتفاع أسعار النطاقات كان عاملاً رئيسيًا في تقليل الأنشطة المخالفة بصورة عامة.[38] كذلك، يتوقع الباحثون من APWG أنه مع زيادة انتشار نطاقات gTLD الجديدة وانخفاض الأسعار بسبب زيادة العرض والمنافسة، فسنرى مزيد من التصيد فيها مقارنة بنطاقات TLD القديمة والخاصة برموز الدول (نطاقات ccTLD). علاوة على ذلك، يظهر أحد الأدلة على هذا في حالة نطاق xyz. الذي عرض نطاقات مجانية لفترة زمنية. وفي النصف الثاني من 2014، تركز ثلثا عمليات التصيد في نطاقات gTLD الجديدة في سجل xyz.[39] بناءً عليه، يبدو أن الحفاظ على انخفاض التكاليف يمثل أحد المخاوف الجوهرية للمتصيدين، حيث أظهرت الدراسة أنه عملاً منخفض المهارات والعائد."[40] من ناحية أخرى، بينما توضح بعض القصص أرباح كبيرة كنتيجة للتصيد، يبدو مع ذلك أن المتصيدين العاديين يمكن أن يحصلوا على ما يعادل بضعة مئات من الدولارات كل أسبوع.[41]

الضمانات التسع

في الطريق نحو برنامج gTLD الجديد، طلبت ICANN النصيحة من الخبراء المتخصصين في إساءة استخدام DNS والأمن الإلكتروني لاقتراح الإجراءات الاستباقية التي يمكن اتخاذها للتخفيف من أنواع الأنشطة المعروضة أعلاه. وقد توصل مجتمع الخبراء إلى الضمانات التسع التالية المعروضة أدناه. ولا يزال الآن على فريق CCT-RT مهمة تحديد درجة تفعيل الضمانات التسع لتحقيق الأهداف المقصودة.

لفهم فاعلية الضمانات التسع في التخفيف من إساءة استخدام DNS، يجب تحديد الفاعلية أولاً كمفهوم قابل للقياس. وستناقش الصفحات التالية هذه التعريفات في سياق كل سؤال مطروح كجزء من الجهود الأولية لأنواع الضمانات التسع التي ستكون لازمة لبرنامج gTLD الجديد. كما سيتم عرض البيانات المتوفرة حول قياسات الفاعلية المقترحة. وفي حالة عدم توفر البيانات، سيتبع ذلك نقاش للأسباب وراء عدم وجود البيانات والوسائل الأخرى المحتملة لتقييم فاعلية الضمانة المحددة.

سؤال: كيف نضمن عدم إدارة أشخاص سيئين للسجلات؟

يمكن فهم الفاعلية في سياق هذا السؤال على أنها منع العناصر السيئة مثل المدانين بجريمة أو جنحة ذات صلة بالأنشطة المالية من تشغيل السجلات. كذلك، في 2001، نصت اتفاقية سجل COM. على إمكانية إنهاء اتفاقية السجل إذا توفر في المشغل أي مما يلي:

---

[37] مجموعة عمل مكافحة التصيّد، "استبيان التصيد العالمي: الاتجاهات واستخدام اسم النطاق، في النصف الثاني من 2015"، 27 مايو 2015، https://apwg.org/apwg-news-center/

[38] افترض أحد المشاركين قيمة حدية أكبر من 15 دولار أمريكي لأي اسم نطاق كالنقطة التي تبدأ عندها معدلات إساءة الاستعمال عامةً في الانخفاض. أبحاث سياسات وعمليات ICANN، "مراجعة ضمانات برامج gTLD الجديد من إساءة استخدام DNS"، 28 يناير 2016، https://newgtlds.icann.org/en/reviews/dns-abuse

[39] كذلك، لاحظ المؤلفون أن معظم عمليات التسجيل للتصيد في نطاق xyz. تمت عبر المشتركين الصينيين واستخدمت لمهاجمة أهداف صينية. راجع مجموعة عمل مكافحة التصيّد، "استبيان التصيد العالمي: الاتجاهات واستخدام اسم النطاق، في النصف الثاني من 2015"، 27 مايو 2015، https://apwg.org/apwg-news-center/

[40] Herley and Florencio, "A Profitless Endeavor: Phishing as Tragedy of the Commons"، أبحاث مايكروسوفت، سبتمبر 2008، http://research.microsoft.com/en-us/um/people/cormac/Papers/PhishingAsTragedy.pdf

[41] المصدر ذاته. يصعب الحصول على البيانات بسبب طبيعتها المخفية. وبالتالي، لا يزال هناك جدال كبير حول التكاليف الفعلية ومزايا التصيد بصورة عامة.

(أ) في حالة إدانته بمعرفة محكمة ذات اختصاص قضائي بجريمة أو جنحة خطيرة ذات صلة بالأنشطة المالية، أو حكمت عليه محكمة مختصة بالاحتيال وخيانة الأمانة، أو وقع عليه بحكم قضائي ترى ICANN بأنه يعادل أي مما سبق بشكل معقول، أو (ب) تعرض لتحديد الإقامة من الحكومة لسلوك يتضمن المشاركة في خيانة أمانة أو إساءة استخدام أموال الآخرين."[42]

كما يوجد هذا البند في اتفاقية سجل gTLD الجديد، بجانب الأحكام الإضافية:

(و) يجوز لـ ICANN، بناء على إشعار مشغل السجل، إنهاء هذا الاتفاق إذا وظف (1) مشغل السجل أي شخص من أرباب السوابق فيما يتصل بالأنشطة المالية أو أي جناية، أو حكم عليه من قبل محكمة مختصة في الاحتيال أو الغش، أو ما هو موضوع قضائي تراه ICANN معقول باعتباره معادلا موضوعيا لأي ضابط لا تنتهي في غضون ثلاثين يوما (30) من معرفة مشغل السجل من إدانة ما سبق، أو (2) لأي عضو من أعضاء مجلس إدارة مشغل السجل أو هيئة حاكمة مشابهة لجناية أو جنحة تتعلق بأنشطة مالية أو أي جناية، أو يتم الحكم فيها من قبل محكمة مختصة بالاحتيال أو خرق واجب الأمانة، أو الخضوع لقرار قضائي تراه ICANN بصورة معقولة معادلا موضوعيا لأي مما سبق وعدم إقالة عضو مجلس الإدارة أو الهيئة الحاكمة الأخرى لدى مشغل السجل في غضون ثلاثين يوما (30) من معرفة مشغل السجل بما سبق.[43]

الضمانة: تدقيق مشغلي السجل

الخلفية

كذلك، تمت إضافة تدقيق عمليات السجل قبل تنفيذ اتفاقية السجل وتفويض نطاق TLD إلى المنطقة الجذر كأحد الضمانات في دليل مقدم طلبات gTLD لبرنامج gTLD الجديد بهدف منع المتقدمين أصحاب السجل الإجرامي أو السلوك المشبوه من تشغيل نطاقات TLD. وقد تم وضع القياس كوسيلة لإنشاء عملية محددة لفحص مشغلي السجلات قبل توقيع اتفاقية السجل أثناء التقييم الأولي للتطبيقات.

شاركت ICANN مع برايس ووترهاوس كوبرز في تنفيذ فحص البيانات الأساسية المركز على مجالين: 1) الاجتهاد التجاري العام، والتاريخ الإجرامي؛ 2) تاريخ سلوك الاحتلال الإلكتروني. وقد تم تناول أهلية طلب محدد للبدء في برنامج gTLD الجديد في التقييم الأولي وفي بعض الأحيان تقارير التقييم الموسعة.

كما تم إجراء فحص البيانات الأساسية المستخدم في برنامج gTLD الجديد في مرحلة زمنية خلال عملية التقييم الأولي. وفي الحالات التي يبلغ فيها مقدم الطلب عن تغييرات في معلومات طلبه في سياق التقييم، يتم إجراء فحص إضافي قبل توقيع اتفاقية السجل. كما تحتفظ ICANN في كافة الحالات بالحق في اتخاذ تدابير العناية الواجبة الإضافية عند اللزوم قبل توقيع أي اتفاقية.

تعريف الفاعلية

بالنسبة للضمانات، يمكن تصور الفاعلية على أنها منع مشغلي السجلات أصحاب السجل الإجرامي أو الضار من التوقيع على اتفاقية سجل مع ICANN. وعلى الرغم من ذلك، كما هو موضح أعلاه، تحدث عملية التدقيق في وقت ويمكن أن تحدث التغييرات في الجهة المسؤولة عن الإدارة لأحد نطاقات TLD (مثلاً، يمكن بيع الشركة أو استبدال المسؤول). وفي سياق إساءة استخدام DNS، من المهم مراعاة ما إذا كان هناك دليل على تشغيل عناصر مخالفة للسجلات أو مخاطر حدوث هذا بصفة مستمرة.

---

[42] "اتفاقية سجل 25 ،"com. مايو 2001، https://www.icann.org/resources/unthemed-pages/registry-agmt-com-2001-05-25-en#II-16C

[43] "اتفاقيات السجل" بتاريخ 9 يناير 2014، https://www.icann.org/resources/pages/registries/registries-agreements-en

السياق الحالي

وفقًا لمراجعة تنفيذ البرنامج المنشورة في يناير 2016، كانت عملية فحص البيانات الأساسية "مراجعة منفذة على كافة الجهات المتقدمة، وكافة الأفراد والمؤسسات المفصح عنها في الأسئلة 9-11، من الطلب، والتي تضمنت المسؤولين والمدراء في هذه الجهات بالإضافة إلى المساهمين المالكين لحصة كبيرة في الجهة."[44] ووفقًا للمراجعة، أجرت ICANN 1150 عملية فحص على 1930 طلب (قدم عدد من الجهات طلبات متعددة). كما تم إبلاغ نتائج فحص البيانات الأساسية لكل طلب عقب اكتمال إجراءات التقييم الأولي. وفي بعض الحالات، تم طرح أسئلة توضيحية على المتقدم وفقًا للجنة فحص البيانات. من ناحية أخرى، اعتبرت مراجعة تنفيذ البرنامج بصورة عامة أن عملية فحص البيانات ناجحة حيث أمكن فحص كافة المتقدمين، إلا أنها لاحظت أن الوقت بين الموعد النهائي لتقديم الطلب وتوقيع اتفاقيات السجل كان أطول من المتوقع. وقد كان هذا يعني أن العديد من المتقدمين كان يلزم إعادة فحصهم. كما أوضحت المراجعة أن عمليات فحص البيانات يمكن إجراؤها في مرحلة التعاقد وليس أثناء التقييم الأولي للحد من الحاجة لإعادة الفحص.

الطرق المحتملة لتجميع البيانات والقياس

قد يكون من المبكر للغاية تحديد فعالية كلا جانبي الضمانة كتدابير وقائية. ويمكن أن يراعي أي إجراء فاعلية البيانات حول عمليات الرفض المستندة إلى فحص البيانات الأولي بالإضافة إلى عمليات الإنهاء لاتفاقيات السجل بسبب فشل السجل في القضاء على العناصر المخالفة من فريق المسؤولين أو مجلس الإدارة. ونظرًا لوجود معلومات شخصية وحساسية عملية فحص البيانات الأساسية، فإن التقارير الموضحة لما إذا كانت الطلبات مؤهلة لبدء الخطوة التالية في العملية محدودة. وعلى الرغم من ذلك، تتوفر الأرقام الكلية. كذلك، يمكن أن تقدم شكاوى الامتثال الرسمية و/أو عمليات إنهاء اتفاقيات السجل مقياسًا لاستمرار فاعلية هذه الضمانة.

إضافة إلى ما تقدم، يمكن أن يكون للضمانة تأثيرًا رادعًا للمتقدمين المحتملين مع بيانات العاملين المشتبه بها. ومع ذلك، يعتبر قياس العامل الرادع، أي عدد الطلبات التي لم تتقدم، شبه مستحيل مع أن هذا التأثير لا يترتب عليه عادةً بيانات قابلة للقياس.

سؤال: كيف نضمن صحة واستخدام معلومات السجل؟

يمكن فهم تحديد الفاعلية فيما يتعلق بهذا السؤال على أنه نجاح استخدام الضمانات للدعم فيما التحقق من معلومات السجل وتأمينها. وفيما يلي ثلاث ضمانات وقائية موضوعة لإنجاز هذا.

الضمانة: طلب خطة موضحة لنشر DNSSEC

الخلفية

تم وضع الملحق الأمني لنظام اسم النطاق (DNSSEC) لإخفاء محاولات العناصر الضارة لاختراق عملية بحث DNS. ويمكن أن تخترق هذه العناصر عمليات بحث مستخدم الويب وعلى سبيل المثال، لتوجيهها إلى مواقع ويب ضارة لسرقة المعلومات السرية. كما تعمل DNSSEC على توفير الحماية ضد هذه الهجمات من خلال توقيع البيانات رقميًا، وبالتالي التأكد من صحتها. فهي توظف التوقيعات المشفرة لسجلات DNS القائمة للتحقق من صحة سجل DNS الناتجة عن خادم الاسم الرسمي ولا تتبدل في أي نقطة.[45] إضافة إلى ذلك، يتيح نشر سجلات DNSSEC للمشتركين تعيين مفاتيح اسم نطاق محددة للنطاقات في حالة اختيارها. وكان تفويض DNSSEC من خلال اتفاقية السجل يهدف إلى ضمان الانتشار الأكبر والأسرع.

---

[44] "مراجعة تنفيذ البرنامج"، 29 يناير 2016، https://www.icann.org/en/system/files/files/program-review-29jan16-en.pdf

[45] "DNSSEC – ما هي ولماذا هي مهمة؟" بتاريخ 1 فبراير 2016، https://www.icann.org/resources/pages/dnssec-qaa-2014-01-29-en؛ "كيفية عمل DNSSEC" بتاريخ 1 فبراير 2016، https://www.cloudflare.com/dnssec/how-dnssec-works/

تتطلب الضمانات وجود خطة محددة لكافة طلبات gTLD الجديدة فيما يتعلق بنشر DNSSEC. ويتم تقييم هذا خلال عملية التقييم الأولي، بهدف الحد من مخاطر سجلات DNS المخادعة. إضافة إلى ذلك، فبموجب اتفاقية السجل، يطلب من مشغلي سجلات gTLD الجديدة توقيع ملفات منطقة TLD مع DNSSEC، واتباع أفضل الممارسات على النحو المبين في RFC رقم 4641 لفريق عمل هندسة الإنترنت وما يخلفه، بجانب قبول المواد العامة الرئيسية من أسماء النطاقات الفرعية بصورة آمنة، ونشر بيانات ممارسات DNSSEC وفقًا للتنسيق الوارد في RFC 6841.[46] [47]

تعريف الفاعلية

يمكن تحديد فاعلية هذه الضمانة بعدة طرق. حيث يمكن تحديدها ببساطة بوجود خطة محددة لدى مشغل السجل لنشر DNSSEC والنجاح في التقييم في مرحلة الطلب. كما يمكن تحديدها وفقًا لعدد المشكلات المبلغ عنها فيما يتعلق بامتثال السجل لمتطلبات DNSSEC. أخيرًا، يمكن تحديدها وفقًا للانتشار الأوسع لامتدادات DNSSEC مثل معدل توقيع المشتركين أو وضع أنظمة حل DNS للتحقق من DNSSEC في الشبكات التي تشغلها مزودو خدمات الإنترنت.[48]

السياق الحالي

اعتبارًا من 23 فبراير 2016، وقع 1073 من 1236 من نطاقات TLD (بما في ذلك ccTLD) في المنطقة الجذر على مفاتيح DNSSEC.[49]

الطرق المحتملة لتجميع البيانات والقياس

يتوفر الآن قياسان وهما عدد نطاقات TLD في المنطقة الجذر وعدد نطاقات المستوى الثاني في كل من هذه المفاتيح الموقعة.[50] كما يمكن أن تركز المزيد من القياسات التفصيلية على قياس مشكلات DNSSEC المكتشفة أثناء اختبار ما قبل التفويض، وعدد مشكلات مراقبة اتفاقيات مستوى الخدمة التي تم الإبلاغ عنها، وعدد الشكاوى المستلمة فيما يتعلق بامتثال DNSSEC.

يجب أن يراعي القياس الشامل للفاعلية في هذا المجال حقيقة أن المشتركين وأمناء السجل ومزودي خدمات استضافة DNS ومزودي خدمات الإنترنت يلعبون جميعًا دورًا رئيسيًا في عملية النشر والعمل الكامل لـ DNSSEC. على سبيل المثال، عندما يطلب من مشغلي السجلات عرض خطة لنشر DNSSEC، فهذا لا يعني توقيع المشتركين عليها بالضرورة. كذلك، توضح البيانات الأولية التي جمعها فريق الخدمات الفنية في ICANN أن نسبة صغيرة عادةً من نطاقات المستوى الثاني وقعت على مفاتيح DNSSEC (بالرغم من أن هذا يختلف بصورة كبيرة حسب TLD).[51] من ناحية أخرى، يمكن أن توجد أحد دراسات الحالة المحتملة هي CloudFlare، شركة خدمات خادم اسم النطاق وتقديم محتوى DNS، التي قررت ترك مهمة تأمين الحركة لأي شخص على الشبكة مع DNSSEC في خطوة واحدة. في هذا الصدد، يمكن أن يسمح أسلوب دراسة الحالة الذي يقدم نظرة شاملة للمجال في دعم DNSSEC من السجلات والمشتركين ومزودي خدمات استضافة DNS ومزودي خدمات

---

[46] اتفاقية سجل ICANN، المواصفة 6: DNSSEC 1.2، بتاريخ 1 فبراير 2016، https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm

[47] RFC هو فئات طلب التعليقات للوثائق الصادرة عن فريق عمل هندسة الإنترنت والتي تتضمن الموجزات الفنية والتنظيمية على شبكة الكمبيوتر والبروتوكولات والإجراءات والمفاهيم. See www.ietf.org/rfc.

[48] "دليل النشر: DNSSEC لمزودي خدمات الإنترنت"، بتاريخ 1 فبراير 2016، http://www.internetsociety.org/deploy360/resources/deployment-guide-dnssec-for-isps/

[49] "تقرير TLD DNSSEC"، بتاريخ 23 فبراير 2016، http://stats.research.icann.org/dns/tld_report/

[50] راجع "تقرير نشر DNSSEC"، بتاريخ 23 فبراير 2016 http://rick.eng.br/dnssecstat/

[51] البيانات التي جمعها فريق الخدمات الفنية في ICANN من ملفات المناطق المتاحة للعامة لأغراض هذا التقرير.

الإنترنت بتحديد مواطن الضعف في نشر DNSSEC عبر نطاقات gTLD. وتتولى مجموعة عمل نشر DNSSEC بالفعل تجميع هذه المعلومات حيث تقدم التقارير على الموقع dnssec-deployment.org.

الضمانة: حظر البدل

الخلفية

تتطلب هذه التوصية عناصر تحكم مناسبة لمنع بدل DNS. ويحدث هذا عندما يستخدم مشغلو السجلات إعادة توجيه DNS أو حروف البدل أو الردود المركبة بدلاً من تقديم رد بخطأ في الاسم للاستفسارات حول DNS غير الموجودة.[52] وقد حظرت ICANN هذه الإجراءات بسبب النتائج التي تظهر أنها تتضمن مخاطر على أمن واستقرار DNS من خلال خلق فرص جديدة للهجمات الضارة.[53]

تم تحديد هذه الضمانة في القسم 2.2 من المواصفات 6 من اتفاقية السجل:

> 2.2. حظر أحرف البدل. بالنسبة لأسماء النطاقات التي لم يتم تسجيلها، أو لم يقدم المسجل سجلات سليمة بشأنها مثل سجلات NS أو ليتضمنها ملف منطقة DND، أو إن كانت حالتهم لا تسمح لهم بنشرهم في DNS، فإنه يحظر استخدام سجلات الموارد العشوائية كما سبق وصفه في RFC رقم 1034 و4592 أو أي وسيلة أو تقنية لموالفة سجلات موارد DNS أو استخدام إعادة التوجيه ضمن DNS من قبل السجل. عند إرسال استعلام بشأن أسماء النطاقات هذه، لا بد أن ترجع خوادم الأسماء المصرح بها الاستجابة "Name Error" (والتي تعرف أيضًا بـ NXDOMAIN)، RCODE 3 كما تم وصفه في RFC 1035 وأرقام RFC ذات الصلة. تنطبق تلك البنود على كل ملفات منطقة DNS على كافة المستويات في هيكل DNS الذي يحتفظ مشغل السجل (أو أي جهة تابعة تعمل في خدمات التسجيل) ببياناته ويرتب لصيانتها، أو توليد العوائد من عمليات الصيانة.

وعلى الرغم من ذلك، تم نشر البدل في 2014، كجزء من إطار عمل إدارة حالات تضارب الأسماء، في بعض نطاقات TLD لفترة محدود عقب تفويض TLD (فترة الانقطاع المتحكم فيه) كوسيلة لتحديد أي حالات تضارب في مساحات الأسماء.[54] كذلك، كما تضمنت المرحلة الأولى من تقرير JAS حول تخفيف مخاطر تضارب مساحة أسماء DNS:

> نوصي بتنفيذ السجل لفترة الانقطاع المتحكم فيه عقب التفويض في المنطقة الجذر وحظر التعليق المؤقت للسجلات بحروف بدل أثناء هذه الفترة. ومع مراعات هدف الانقطاع المتحكم فيه وحقيقة عدم وجود بيانات مشتركين في هذه المنطقة، نرى أن السماح المؤقت بسجلات حروف البدل لهذا الغرض لا

---

[52] "حول حظر أحرف البدل (إعادة توجيه النطاق)"، بتاريخ 1 فبراير 2016، https://www.icann.org/resources/pages/wildcard-prohibition-2014-01-29-en

[53] اللجنة الاستشارية للأمان والاستقرار التابعة لـ ICANN، "SAC041: توصية لحظر استخدام إعادة التوجيه والرد المصطنع من TLDs الجديدة، 10 يونيو 2009، https://www.icann.org/en/system/files/files/sac-041-en.pdf

[54] راجع "الأسئلة المتداولة: إطار عمل إدارة حالات تضارب الأسماء للسجلات"، بتاريخ 11 فبراير 2016، www.icann.org/resources/pages/name-collision-ro-faqs-2014-08-01-en، والذي ينص على ما يلي: "يسقط الحظر المفروض على أحرف البدل بالنسبة لفترة الانقطاع المسيطر عليه لنطاقات المستوى الأعلى المعمول بها (أي، حيث لا توجد أسماء نشطة تحت TLD بخلاف "مركز معلومات الشبكة"). ولا ينطبق هذا التنازل إلا في حالة عدم وجود أسماء مفوضة (وبالتالي، التشغيلية) داخل TLD تلك، والتي تزيل المخاطر التي ترتبط على نحو تقليدي بتطبيقات أحرف البدل. ويرجع سبب رفع الحظر وتحديد استخدام أحرف البدل لالتقاط جميع حالات تضارب الأسماء الواضحة. وستطابق أحرف البدل في "أعلى" النطاق كل الاستعلامات التي سوف تظهر أكثر من أي وقت مضى بمجرد أن يعمل النطاق بكامل طاقته. كما يزيد هذا النهج إلى أقصى درجة من الخطوات المتخذة لحماية مستخدمي الإنترنت الذين يسربون حاليا الاستفسارات التي يراد لها أن تكون محلية."

تتعارض مع عمليات حظر ICANN المحددة حول السجلات بحروف البدل ولا يطرح أي مخاوف تتسبب في وضع ICANN لهذه المحظورات.[55]

تعريف الفاعلية

بالنسبة لهذا الإجراء، يمكن تحديد الفاعلية نظريًا من حيث درجة الامتثال لحظر حروف البدل في نطاقات gTLD الجديدة. كما تمكن مراعاة تقييم هذا السلوك كوسيلة لضمان نزاهة واستخدام معلومات السجل. ويمكن أيضًا تقييم المساهمات فيما يتعلق بالتأثير على السلوكيات التي تسعى هذه الضمانة لمنعها.

السياق الحالي

تتيح ICANN "نموذج الامتثال لحظر البدل (إعادة توجيه النطاق)" للسماح بإصدار تقارير عدم الامتثال للأحكام التعاقدية.[56] وحتى تاريخه، لم تتلقى ICANN أي شكاوى حول حظر البدل من خلال هذه الأداة.[57]

الطرق المحتملة لتجميع البيانات والقياس

كما أشرنا أعلاه، لم تستلم أية شكاوى فيما يتعلق بالبدل من سجلات gTLD الجديدة. ويمكن أن يكون الاستفسار النوعي من الخبراء المتخصصين حول فاعلية هذه الضمانة وسيلة للتحايل على عدم وجود البيانات النوعية.

كما يمكن أن تتضمن الأساليب الأخرى عدم النظر فقط في الشكاوى إلى ICANN حول الفشل في حظر البدل في نطاقات TLD محددة، ولكن أيضًا الانتشار الحالي لاستخدام إعادة توجيه مستخدمي DNS إلى خوادم الويب المعتمدة على الإعلانات عند فشل بحث DNS. تمثل ICSI Netalyzr من بيركلي بجامعة كاليفورنيا أحد أدوات فحص الشبكات كما أنها جزء من دراسة القياس التي تعمل على قياس سلامة الإنترنت. كما أنها استخدمت في العديد من الدراسات التي تفحص مشكلات إعادة توجيه DNS وربما تكون أداة مفيدة فهم آثار البدل في DNS.[58]

الضمانة: استبعاد السجلات المتبقية الوحيدة

الخلفية

تم وضع هذه الضمانة للحد من مخاطر العناصر الضارة المتسللة بروابط إلى النطاقات الضارة في المنطقة الجذر عن طريق السجلات المتبقية الوحيدة وهي سجلات خادم الاسم التي يمكن أن تبقى بمجرد استبعاد السجل الأصلي من المنطقة. ويمكن أن تتيح السجلات المتبقية الوحيدة للعناصر الضارة السيطرة على خوادم الأسماء، التي توفر لها بعد ذلك القدرة على تنفيذ الأنشطة الضارة من النطاقات القانونية في ظاهرها. على سبيل المثال، تعرف هجمات التمويه السريع بأنها تستفيد من السجلات المتبقية الوحيدة في استضافة النطاقات الضارة لفترات زمنية قصيرة.[59]

---

[55] JAS Global Advisors، "الحد من مخاطر تضارب أسماء نطاقات نظام DNS"، بتاريخ 4 يونيو 2014، https://www.icann.org/en/system/files/files/name-collision-mitigation-study-06jun14-en.pdf

[56] راجع "نموذج الامتثال لحظر البدل (إعادة توجيه النطاق)"، بتاريخ 11 فبراير 2016 https://forms.icann.org/en/resources/compliance/registries/wildcard-prohibition/form

[57] على الرغم من ذلك، كانت هناك بعض الشكاوى المتعلقة بالامتثال في "الأسماء المحتفظ بها/الانقطاع المتحكم به." راجع "لوحة معلومات الامتثال التعاقدي في ICANN لسنة 2016"، بتاريخ 12 فبراير 2016، https://features.icann.org/compliance/dashboard/0116/report

[58] Weaver, Kreibich, and Paxson, "Redirecting DNS for Ads and Profit," USENIX Workshop on Free and Open Communications on the Internet (FOCI), 2011, http://www.icir.org/christian/publications/2011-foci-dns.pdf

[59] راجع اللجنة الاستشارية للأمان والاستقرار (SSAC) التابعة لـ ICANN، استشارة استضافة التمويه السريع وDNS، مارس 2008، https://www.icann.org/en/system/files/files/sac-025-en.pdf

تتطلب الضمانة أن يقدم مشغلو السجلات خطة في طلبهم لاستبعاد السجلات المتبقية الوحيدة بمجرد استبعاد السجل الأصلي. وبمجرد الالتزام بشروط اتفاقية السجل يطلب من مشغلي السجل مراعاة استبعاد السجلات المتبقية الوحيدة حسب المادة 6، البند 4.2 من الاتفاقية والذي ينص على ما يلي: "يلتزم مشغل السجل باتخاذ إجراء للتخلص من سجلات الملصق المعزولة... عند التزويد بأدلة في شكل مكتوب على أن هذه السجلات موجودة فيما يتعلق بالسلوك الخبيث."[60]

تعريف الفاعلية

بالنسبة لهذا الإجراء، يمكن فهم الفاعلية على أنها ممارسات منتظمة من جانب السجلات لتقديم جهات اتصال للمستخدمين النهائيين للإبلاغ عن المخالفات وتأكيد الاستبعاد التلقائي للسجلات المتبقية الوحيدة عند استبعاد السجل الأصلي من المنطقة.

السياق الحالي

توضح تعليقات المجتمع الأولية حول هذه المشكلة أن السجلات المتبقية الوحيدة هي أحد مصادر المخالفات التي تم تحييدها بصورة كبيرة من خلال الاستبعاد المنتظم لها من ملفات المنطقة، بالرغم من بقائها مشكلة منخفضة المستوى في بعض الحالات.[61]

الطرق المحتملة لتجميع البيانات والقياس

تلقت ICANN بعض التعليقات الأولية التي تقترح إمكانية قياس هذه الضمانة باستخدام ملفات المنطقة لتتبع استبعاد السجلات المتبقية الوحيدة مع الوقت.

في هذا الصدد، يمكن أن تقدم مناقشة انتشار واستخدام السجلات المتبقية الوحيدة لأغراض ضارة لدى مشغلي السجل قياسًا نوعيًا لفعالية استخدام السجلات والمشتركين وأمناء السجل للآليات اللازمة لاستبعاد هذا النوع من السجلات. كما يمكن اعتبار الدليل المكتوب اللازم لمشغل السجل لاستبعاد السجلات المتبقية الوحيدة وفقًا لنص المادة 6 كمصدر مفيد للبيانات. كذلك، يمكن أن يفيد أيضًا تحديد موقع حالات التوصيات لاستبعاد السجلات المتبقية الوحيدة في سياسات مكافحة المخالفات في السجلات. على سبيل المثال، يتضمن نطاق المستوى الأعلى rich. قسمًا يركز على استبعاد السجلات المتبقية الفردية في سياسة مكافحة المخالفات،[62] مع تركيز Afilias على هذه المشكلة كأحد عناصر استضافة التمويه السريع.[63]

سؤال: كيف نضمن تركيز الجهود أكثر على مكافحة المخالفات المحددة؟

يركز هذا السؤال على توفر المعلومات لتقليص الأنشطة ودعم تحديد المخالفين في DNS.

الضمانة: مطلب لسجلات WHOIS المفصلة

الخلفية

تتطلب هذه الضمانة أن تحتفظ نطاقات gTLD الجديدة بسجلات WHOIS "الوافرة" وتمنح الوصول إليها، وذلك لتحسين توفر وكمال بيانات WHOIS. وتمثل سجلات WHOIS المفصلة هي السجلات التي تتضمن معلومات

---

[60] راجع تعليقات اللجنة الاستشارية للأمن والاستقرار في ICANN حول السجلات المتبقية الوحيدة في مسودة دليل مقدم الطلب"، مايو 2011، https://www.icann.org/en/system/files/files/sac-048-en.pdf

[61] أبحاث سياسات وعمليات ICANN، "مراجعة ضمانات برامج gTLD الجديد من إساءة استخدام DNS"، 28 يناير 2016، https://newgtlds.icann.org/en/reviews/dns-abuse

[62] "سياسة مكافحة المخالفات في RICH."، بتاريخ 11 فبراير 2016، http://nic.rich/files/policies/rich-anti-abuse-policy.pdf

[63] "سياسة مكافحة المخالفات في Afilias"، بتاريخ 11 فبراير 2016، http://dotblue.blue/about/afilias-anti-abuse-policy

الاتصال الخاصة بالمسجل ومعلومات الاتصال الإدارية والفنية المخصصة، بالإضافة إلى أي من السجل الراعي ومعلومات حالة التسجيل."[64] على الجانب الآخر، يتعارض هذا مع سجلات WHOIS المختصرة، التي تخزن فقط المعلومات الكافية لتحديد أمين السجل المتعهد وحالة التسجيل ولا تقدم أي معلومات حول المشترك. كذلك، يمكن أن يتيح استخدام سجلات WHOIS المفصّلة بحث بيانات أكثر اكتمالاً وسرعة في معرض جهود تحديد العناصر الضارة التي تعمل في DNS.

تعريف الفاعلية

بالنسبة لهذا الإجراء، يمكن تحديد الفاعلية من خلال وضع مجموعة من سجلات WHOIS المفصّلة المستخدمة بانتظام من قبل السلطات لتتبع وتحديد وتقليص أنشطة العناصر الضارة في DNS.

السياق الحالي

يطلب من كل مشغل سجل gTLD جديد لديه تفويض لنطاقات TLD في المنطقة الجذر إنشاء والاحتفاظ بسجلات WHOIS مفصلة كجزء من التزاماته التعاقدية.

الطرق المحتملة لتجميع البيانات والقياس

يتمثل المقصد في النص على احتفاظ سجلات gTLD الجديدة بسجلات WHOIS المفصّلة في إنشاء مجموعة شاملة أكثر لسجلات العقود حتى تتيح للسلطات تتبع الأنشطة الضارة وإيقافها. كما يمكن أن يكون الحصول على تعليقات من المستجيبين لمخالفات DNS فيما يتعلق باستخدام سجلات WHOIS المفصلة مقابل المختصرة في تقليص إساءة استخدام DNS أحد وسائل تقييم فاعلية هذه الضمانة.

يمكن أن تنتج القياسات المحتملة الأخرى من البيانات الناتجة عن نظام تقارير دقة WHOIS، والتي تمثل أحد مشروعات التنمية الحالية التي تهدف إلى تحديد ورفع التقارير حول الدقة بانتظام لتحسين جودة بيانات الاتصال في WHOIS".[65] كذلك، تلخص المخططات التالية من تقرير المرحلة الثانية المنشور في ديسمبر 2015 دقة gTLD الشاملة فيما يتعلق بمتطلبات بنية اتفاقية اعتماد أمناء السجل لسنة 2009 حسب الوضع ودقة gTLD الشاملة لمتطلبات عمل اتفاقية اعتماد أمناء السجل لسنة 2009 حسب الوضع:[66]

دقة نطاقات gTLD الإجمالية مع متطلبات التركيب اللغوية لاتفاقية RAA لسنة 2009 بحسب وضع العقد

	البريد الإلكتروني	الهاتف	العنوان البريدي	الثلاث دقيقة جميعًا
الثلاث جهات دقيقة جميعًا	%0.2 ± %99.1	%0.7 ± %83.3	%0.8 ± %79.4	%0.9 ± %67.2

دقة نطاقات gTLD الإجمالية مع متطلبات العمل لاتفاقية RAA لسنة 2009 بحسب وضع العقد

	البريد الإلكتروني	الهاتف	العنوان البريدي	الثلاث دقيقة جميعًا
الثلاث جهات دقيقة جميعًا	%0.7 ± %87.1	%0.9 ± %74.0	%0.3 ± %98.0	%0.9 ± %64.7

---

[64] ICANN WHOIS, "WHOIS Primer"، بتاريخ 11 فبراير 2016، https://whois.icann.org/en/primer

[65] لاحظ أن المرحلة 3 من الدراسة لم تنفذ بعد، ولكنها ستركز على "متطلبات الهوية"، التي تفحص ما إذا كانت جهة الاتصال المطروحة هي بالفعل الفرد أو الجهة المسؤولة عن النطاق. كما تعرف متطلبات البنية على أنها تنسيق قيد WHOIS. وتعرف متطلبات العمل على أنها قدرة العقود على تحديد المستخدم والاتصال به. كذلك، لاحظ أنه بينما تكون بعض العقود قابلة للعمل والاتصال بالمستخدم، لا تفحص ARS ما إذا كان المستخدم هو المبين في سجل WHOIS. راجع "تقرير المرحلة 2 الدورة 1 من WHOIS ARS: دقة البنية والعمل"، بتاريخ 1 فبراير 2016، https://whois.icann.org/en/file/whois-ars-phase-2-cycle-1-report-syntax-and-operability-accuracy و"نظام تقارير دقة WHOIS"، بتاريخ 11 فبراير 2016، https://whois.icann.org/en/whoisars

[66] المصدر ذاته.

قد تقدم المراحل الثلاث لدراسة WHOIS ARS، التي تركز على البنية والدقة والسريان على التوالي، مجموعة من قياس الوكيل لفاعلية هذه الضمانة. ومن الناحية النظرية، ستوفر سجلات WHOIS الأدق لمجتمع مكافحة المخالفات أداة مفيدة لمكافحة إساءة استخدام DNS. وعلى الرغم من ذلك، لا يمكن أن تقدم العناصر الضارة مسبقًا تفاصيل دقيقة للعقد. ولا يزال على فريق CCT-RT مهمة تحديد ما إذا كانت "البنية والدقة والسريان" مؤشرات مناسبة للفاعلية في هذا المجال.

الضمانة: مركزية الوصول إلى ملف المنطقة

الخلفية

تتطلب هذه الضمانة توفير بيانات اعتماد الوصول للحصول على بيانات ملف منطقة السجل عبر مصدر مركزي، مما يتيح لمجتمع مكافحة المخالفات الحصول على المستجدات حول النطاقات الجديدة داخل كل منطقة TLD بشكل أكثر كفاءة. ويقصد من هذا تقليل الوقت اللازم لاتخاذ إجراء تصحيحي داخل نطاقات TLD التي تتعرض لنشاط ضار.

تعريف الفاعلية

بالنسبة لهذه الضمانة، يمكن تحديد الفاعلية حسب قدرة خدمات بيانات المنطقة المركزية على معالجة طلبات بيانات ملف منطقة الجذر بفاعلية في الوقت المحدد للحد من أوقات الاستجابة في مكافحة الأنشطة الضارة.

السياق الحالي

تكون سجلات gTLD الجديدة مطلوبة بموجب المواصفة 4، القسم 2 من اتفاقية سجلات gTLD لتوفير بيانات منطقة للمستخدمين النهائيين اللذين طلبوها. وتوضح تقارير ICANN المتاحة علنًا اعتماد أكثر من 3 مليون كلمة مرور للوصول لملف المنطقة في عام 2015 فقط.[67] كما توضح الحوارات مع الباحثين الأمنيين لأغراض هذا التقرير أن CZDS تقدم خدمات قيمة للمستجيبين لإساءة استخدام DNS وللذين يسعون لحماية ملكيتهم الفكرية. ومع ذلك، بينما وضعت CZDS مع هذا الغرض تنفيذ عملية لتوفير الوصول إلى ملفات المنطقة بكفاءة أكبر، فقد أبلغت السجلات نفسها عن انتشار الإحباط من الخدمة.[68] ولا يزال على مشغلي السجلات التحقق من بيانات المستخدم النهائي ولا تحد اتفاقية السجل من الوقت الذي يجب خلاله أن يستجيب مشغلو السجلات لطلبات الوصول. على أن هذا يترتب عليه عادةً تكدس كميات لا تمكن إدارتها من الطلبات لمشغلي السجل وعدم وجود القدرات اللازمة من جانبهم للاستجابة للطلبات في الوقت المحدد. في هذا الصدد، أبلغ أحد ممثلي السجلات عن استلامه 7-10 آلاف طلب للوصول إلى ملف المنطقة يوميًا.[69] ويمكن أن يترتب على هذا عدم الإنفاذ الكامل لشروط الاستخدام والتحقق العاجل لبيانات اعتماد الطالب.[70] كما حدد امتثال ICANN طلب الجهات الخارجية للوصول إلى ملف المنطقة من خلال CZDS كأحد أهم المشكلات في امتثال السجل لسنة 2015، حيث كانت معظم الشكاوى متعلقة بعدم استجابة مشغلي السجلات للطلبات بالوصول إلى ملف المنطقة ومنع مشغلي السجلات الوصول لأسباب لا تسمح بها اتفاقية السجل.[71]

---

[67] تقارير كلمات المرور الشهرية CZDS ZFA، بتاريخ 1 فبراير 2016، https://czds.icann.org/en/reports

[68] أبحاث سياسات وعمليات ICANN، "مراجعة ضمانات برامج gTLD الجديد من إساءة استخدام DNS"، 28 يناير 2016، https://newgtlds.icann.org/en/reviews/dns-abuse

[69] المصدر ذاته.

[70] المصدر ذاته.

[71] "ICANN، الامتثال التعاقدي - التقرير السنوي لعام 2015"، يناير 2016 https://www.icann.org/en/system/files/files/annual-2015-27jan16-en.pdf

الطرق المحتملة لتجميع البيانات والقياس

يمكن قياس أحد مؤشرات الفاعلية من خلال تقارير كلمات مرور CZDS التي توضح عدد كلمات مرور ZDA (المقدمة للمستخدمين الذين طلبوا الوصول إلى ملفات المنطقة بالجملة) في CZDS وعدد كلمات المرور المعتمدة كل شهر في نطاقات TLD المحددة وبصورة عامة.[72] وقد تقدم تعليقات المستخدمين حول الخدمة تفاصيل إضافية لهذا القياس حيث يبلغ العديد من المستخدمين عن مشكلات في التعامل مع طلبات CZDS على الأقل وفقًا لما هو متناقل.

الضمانة: توثيق اتصالات وإجراءات إساءة الاستخدام على مستوى السجل

الخلفية

تتطلب هذه الضمانة من مشغلي السجل إنشاء نقطة اتصال واحدة مسؤولة عن معالجة شكاوى إساءة الاستخدام. كما توجه أدلة التقديم المتقدمين بإنشاء خطة التنفيذ لإنشاء ونشر نقطة الانتهاك المخصصة للاتصال والمسؤولة عن معالجة المسائل التي تتطلب اهتماما عاجلاً، وتوفير الاستجابة في الوقت المناسب لشكاوى إساءة الاستخدام...".[73] في هذا الصدد، تنص الفقرة 6 من القسم 4.1 من اتفاقية السجل على ما يلي: "يقدم مشغل السجل لـ ICANN وينشر على موقعه الإلكتروني تفاصيل اتصال دقيقة تتضمن بريد إلكتروني سليم وعنوان بريد صحيح وأيضًا الشخص المسئول الرئيسي عن التعامل مع الاستعلامات الخاصة بإساءة التعامل مع TLD، ويقدم إلى ICANN إشعارًا سريعًا بأي تغييرات تطرأ على معلومات الاتصال هذه."[74]

تعريف الفاعلية

بالنسبة لهذا الإجراء، يمكن قياس الفاعلية حسب توفر هذه المعلومات للمستخدمين النهائيين والعثور على طريقة لقياس السهولة النسبية التي يمكن للمستخدم بها الإبلاغ عن إساءة استخدام DNS. ويمكن أن يتمثل الأسلوب التكميلي في مقابلة سلطات إنفاذ القانون ومشغلي السجلات أنفسهم للحصول على تعليقاتهم بشأن فاعلية هذا الإجراء.

السياق الحالي

راقب الامتثال في ICANN معلومات جهة اتصال المخالفات المطلوب من السجلات نشرها على مواقع الويب والتي تنص على ما يلي في آخر تحديث للامتثال التعاقدي لمراجعة المشكلة:

> واصلت ICANN مراقبتها الوقائية لمعلومات جهة اتصال إساءة الاستخدام التي يتعين على السجلات بموجب اتفاقية السجل الجديدة نشرها على موقع الويب الخاصة بهم. ومن خلال القيام بذلك، تضمن ICANN أن المستخدمين النهائيين، بما في ذلك على سبيل المثال لا الحصر وكالات إنفاذ القانون، يصلون إلى نقطة اتصال من أجل الإبلاغ عن الأنشطة الضارة في نطاقات TLD... كما راجعت ICANN موقع ويب لعدد 64 نطاق من المستوى الأعلى والتي بدأت فترة الدعاوى بين 1 يناير 2015 و31 مارس 2015. وكان عدد استعلامات عدم الالتزام أو الإشعارات المقدمة إلى السجلات أقل في الجولة السابقة من المراقبة. وكان من بين أوجه القصور التي لوحظت ما يلي: عدم عرض المعلومات المطلوبة على الإطلاق، أو فقد جهة الاتصال الرئيسية، أو فقد عنوان المراسلة لتقارير إساءة الاستخدام. وتتعاون ICANN مع السجلات من أجل تصحيح ما يتم التعرف عليه من عدم توافق.[75]

---

[72] تقارير كلمات المرور الشهرية-CZDS ZFA، بتاريخ 1 فبراير 2016، https://czds.icann.org/en/reports

[73] "دليل المتقدمين لسجلات gTLD"، 4 يونيو 2012، https://newgtlds.icann.org/en/applicants/agb

[74] "اتفاقيات السجل" بتاريخ 9 يناير 2014، https://www.icann.org/resources/pages/registries/registries-agreements-en

[75] راجع "مستجدات الالتزام التعاقدي في ICANN، يناير - مارس 2015"، https://www.icann.org/en/system/files/files/compliance-update-mar15-en.pdf

توضح بعض تعليقات المجتمع الأولية حول هذه الضمانة أن جهات الاتصال للمخالفة تم استخدامها غالبًا من قبل مرسلي البريد غير المرغوب فيه.[76]

الطرق المحتملة لتجميع البيانات والقياس

يمكن أن يكون تحليل تقارير امتثال ICANN وشهادات مستخدمي جهات الاتصال أسلوبًا لقياس فاعلية هذه الضمانة. ويمكن أن تتضمن الطريقة الأخرى تجميع معلومات اتصال مخالفات السجل واختبار عملها.

الضمانة: المشاركة في عملية طلب أمان السجل المرسل (ERSR)

الخلفية

توفر هذه الضمانة آلية تتيح لمشغلي السجلات اتخاذ إجراءات سريعة وحاسمة في ضوء التهديدات التي يتعرض لها نظام اسم النطاق (DNS) من خلال وضع عملية مخصصة لمراجعة طلبات الأمان المرسلة والموافقة عليها. ومن الناحية العملية، يسمح للسجلات طلب التخلي التعاقدي عبارة عن إعفاء من التوافق مع فقرة محددة لاتفاقية السجل لفترة من الوقت ضرورية للاستجابة للتهديدات الأمنية. وقد تم وضعه ليوفر الأمن التشغيلي فيما يتعلق بالتهديدات مع استمرار إخطار الأطراف المعنية بحالة التهديد. لاحظ أن هذه العملية وضعت كاستجابة لفيروس كونفيكر وبالتالي، قبل العمل على تحديد ضمانات برنامج gTLD الجديد. لذا، فلم تدرج في اتفاقية السجل الأخيرة، إلا أنها تتوفر كعملية في السجلات مع حاجة واضحة وقائمة لها.[77]

تعريف الفاعلية

يمكن تصور الفاعلية على أنها السرعة التي تم تحديد التهديد الأمني بها وتحييده كنتيجة ERSR.

السياق الحالي

نظراً للطبيعة الحساسة للبيانات، لا تقدم ICANN تقارير علنية حول تفاصيل هذه العملية. ومع ذلك، توضح المساهمات الأولية من الباحثين الأمنيين لأغراض هذا التقرير أن الضمانة استخدمت استخدامًا فعالاً منذ ظهور فيروس كونفيكر وذلك لحل شبكات بوتنت اللاحقة.

الطرق المحتملة لتجميع البيانات والقياس

لفهم فاعلية هذا الإجراء، يمكن تجميع تعقيبات من طلبوا إجراء عملية ERSR لفهم قدرتها على التعامل مع التهديدات الأمنية. ونظرًا للعدد المحدود لطلبات ERSR وحساسية البيانات الأمنية المتأصلة في العملية، يمكن توجيه التركيز التحليلي إلى كيفية تنفيذ العملية، مثل السرعة والسهولة النسبية للتعامل مع التهديد كنتيجة لـ ERSR، وليس عدد حالات طلب ERSR أو خصائص كيفية مواجهة التهديدات الأمنية.

سؤال: كيف نقدم إطار مراقبة محسن لنطاقات TLD مع احتمالية فعلية لوجود سلوك ضار؟

الضمانة: إنشاء مسودة إطار لبرنامج لتحقق من المنطقة عالية الأمان

الخلفية

اقترحت هذه التوصية، لم تحدد أبدًا رسميًا في اتفاقية السجل كضمانة مطلوبة أو تدرج كمبادرة رسمية تدعمها ICANN، إنشاء برنامج تطوعي لمشغلي السجل الراغبين في إنشاء وإثبات مستوى محسن من الأمن والثقة في

---

[76] أبحاث سياسات وعمليات ICANN، "مراجعة ضمانات برامج gTLD الجديد من إساءة استخدام DNS"، 28 يناير 2016، https://newgtlds.icann.org/en/reviews/dns-abuse

[77] "التقرير النهائي لمجموعة عمل سياسات إساءة استخدام التسجيل"، مايو 2010 http://gnso.icann.org/en/issues/rap/rap-wg-final-report-29may10-en.pdf

نطاقات TLD. وكان الهدف الكلي من البرنامج هو تقديم مجموعة ممارسات موحدة للسجلات التي تسعى للتميز في هذه المجالات.[78]

تعريف الفاعلية

بالنسبة لهذا الإجراء، يمكن النظر إلى الفاعلية على أنها نجاح الاعتماد والتنفيذ والتحقق لمنطقة أمنية حساسة في نطاق TLD مع احتمالية مرتفعة لوجود نشاط ضار (مثلاً تلك التي تمثل القطاعات المصرفية أو المالية أو الدوائية).

السياق الحالي

بينما لا توجد مسودة إطار شامل لبرنامج مماثل عبر مختلف آليات وضع السياسات وتنفيذها في ICANN، استهدفت بعض الجهود التعامل مع تزايد الاحتياجات الأمنية لبعض السلاسل.

وخلال عملية الطلب لنطاق gTLD جديد، تم تقييم السياسات الأمنية للمتقدمين فيما يتعلق بالسلاسل الحساسة، بموجب إرشادات السؤال 30 من دليل مقدم الطلب الذي يطلب من المتقدمين

> تقديم ملخص للسياسة الأمنية للسجل المقترح، بما في ذلك على سبيل المثال لا الحصر، (أ) وصف أي زيادة لمستويات الأمان أو قدرات تتناسب مع طبيعة طلب الحصول على سلسلة TLD، بما في ذلك تحديد أي معايير الدولية القائمة أو صناعة الأمن ذات الصلة بما يلتزم مع مقدم الطلب التالي...[79]

إضافة إلى ذلك، أوصت اللجنة الاستشارية الحكومية في ICANN بإنشاء نموذج للتحقق من بيانات اعتماد مشغلي السجلات كالتزامات المصلحة العامة في القطاعات عالية التنظيم بهدف إنشاء والاحتفاظ بالثقة في هذه النطاقات.[80]

ظهر أيضًا عدد من الجهود المستقلة لزيادة الأمن والثقة في نطاقات gTLD الجديدة من جانب المؤسسات والسجلات المعنية. على سبيل المثال، يعمل سجل شركة fTLD Service, LLC، بصورة مستقلة على إنشاء منطقة عالية الأمن لنطاقات TLD لديها "bank." و"insurance.".[81] في هذا الصدد، يعمل مشروع إحكام DNS على بناء الثقة في مجال اسم النطاق من خلال التنظيم الذاتي وتحديد أفضل الممارسات لمساعدة مستخدمي الإنترنت على تحديد مواقع الويب الموثوقة.[82]

الطرق المحتملة لتجميع البيانات والقياس

يمكن أن يعمل تجميع التعليقات من مشغلي السجلات حول أسباب اختيار عد تتبع التحقق من HSZ على تقديم رؤية إلى عدم اعتماد الضمانة الموصى بها. كذلك، يمكن أن يمثل الحديث مع سجل fTLD Service, LLC حول سبب اختيار تتبع HSZ الخاصة به أحد مصادر البيانات الإضافية.

---

[78] icann.org، "التعليقات العامة: التقرير النهائي لنطاق TLD للمنطقة الأمنية الحساسة"، 11 مارس 2011، https://www.icann.org/news/announcement-2011-03-11-en

[79] "دليل المتقدمين لسجلات gTLD"، 4 يونيو 2012، https://newgtlds.icann.org/en/applicants/agb

[80] راجع "بيان GAC، بيونس آيريس، الأرجنتين"، بتاريخ 24 يونيو 2015، https://www.icann.org/news/announcement-2-2015-06-24-en
و"بيان GAC، دبلن، أيرلندا"، بتاريخ 21 أكتوبر 2015، https://www.icann.org/news/announcement-2015-10-22-en

[81] راجع خدمات سجل fTLD، "الأمن المحسن"، بتاريخ 11 فبراير 2016 www.ftld.com/enhanced-security/

[82] "نبذة عن مشاريع إحكام DNS"، بتاريخ 12 فبراير 2016، http://dnsseal.wiki/About_the_DNS_Seal_Project

العروض والنماذج البحثية

تظهر الألغاز التطبيقية الكبيرة فيما يتعلق بالعلاقة بين توسعة DNS من خلال برنامج gTLD الجديد وانتشار السلوك المخالف الإجرامي في DNS. وتبقى الأسئلة المهمة متعلقة بمساهمة برنامج gTLD الجديد في زيادة إساءة استخدام DNS المتناسبة مع الزيادة في حجم DNS كنتيجة للبرنامج، وكذلك فيما يتعلق بتفعيل الضمانات لتلافيها لتكون فعالة في تحقيق الأهداف المقصودة منها. ومع ذلك، ركز الهيكل الحالي للمراجع على نشر إساءة استعمال DNS حصريًا من خلال الدراسات المعتمدة على الإحصاءات التوضيحية وركزت على تدقيق أنشطة إساءة استخدام DNS كما أنها تعاني من نقص واضح في الدراسات الطولية واسعة التركيز التي تستخدم التحليلات الإحصائية الاستنتاجية متعددة المتغيرات.

إضافة إلى ما تقدم، للوصول إلى صورة شاملة لوضع إساءة استخدام DNS في نطاقات gTLD الجديدة وتقييم فاعلية الضمانات لتلافيها، يعرض هذا التقرير تحليلاً عابرًا معتمدًا على الافتراضات باستخدام الضمانات كمتغيرات تدخل في مجموعة من النماذج الافتراضية المعتمدة على الافتراضات المعقولة فيما يتعلق بالعلاقة بين ضمانات برنامج gTLD الجديد وانتشار السلوك المخالف في DNS. ويركز النموذج على الإجابة على سؤال بحثي مركزي:

> إلى أي درجة يمكن أن تؤثر الضمانات المعمول بها لتلافي إساءة استخدام DNS في نطاقات gTLD الجديدة على السلوك المخالف في DNS؟

ولإجابة هذا السؤال بصورة شاملة وواضحة علميًا، يجب وضع نموذج افتراضي قابل للاختبار وتقسيم الاستفسار للتركيز على نطاقات TLD القديمة والجديدة، أو مساحة DNS بالكامل عندما يكون ذلك مناسبًا. كما يتطلب هذا إنشاء قياس أساسي كنقطة خروج عند الإجابة على السؤال الأساسي المتعلق بما إذا كانت هناك زيادة في إساءة استخدام DNS كنتيجة لبرنامج gTLD الجديد المتناسب مع توسعة DNS نفسه. وبمجرد إنشاء هذا القياس، يمكننا البدء في طرح الأسئلة التي تركز على معدلات إساءة الاستخدام في فترة ما قبل الضمانة مقارنة بفترة الضمانة لتوسع DNS. كما يتيح هذا للباحثين فهم سياق العلاقة المحتملة بين الضمانات التسع والمعدل الحالي لإساء استخدام DNS.[83]

تتعامل النماذج أدناه مع طرق الفحص الكمية والنوعية. ومع ذلك، لا يترتب على العديد من إجراءات الضمانة إنشاء بيانات كمية في الكميات اللازمة لإجراء تحليل إحصائي شامل، كما هو مشار إليه أعلاه. في هذا الصدد، يمكن التعامل مع هذا بأسلوبين: استعراض قياسات الوكيل المحتملة لفاعلية الضمانات، واستخدام الطرق النوعية، مثل مقابلات تعليقات المستخدم ومجموعات التركيز ومراجعة المنشورات ذات الصلة، لإضافة عمق تجريبي للنطاق الأوسع للطرق الكمية المتاحة في سياق الضمانات.

إطار كمي محتمل لاختبار فاعلية الضمانات

يعرض المقترح والنماذج أدناه الخطوات الأولى للإخطار بالنقاش حول أكثر الوسائل الفعالة لاختبار فاعلية الضمانات للحد من إساءة استخدام DNS. ولا يزال على فريق CCT-RT مهمة تحديد ما إذا كان نطاق وبنية الاستفسار فيما يتعلق بجهود التخفيف من إساءة استخدام DNS.

---

[83] لاحظ أن هذا الأسلوب لمقارنة معدل إساءة الاستخدام في نطاقات TLD القديمة سواء حاليًا أو خلال فترة ما قبل gTLD الجديد مع طرح إساءة الاستخدام في نطاقات gTLD الجديدة بصورة مستقلة وتفضيلها من قبل عدد من المشاركين في جلسة المؤتمر الهاتفي فيما يتعلق بقياس إساءة استخدام DNS وفاعلية الضمانات التسع. راجع أبحاث سياسات وعمليات ICANN، "مراجعة ضمانات برامج gTLD الجديد من إساءة استخدام DNS"، 28 يناير 2016، https://newgtlds.icann.org/en/reviews/dns-abuse

تصميم البحث: الأسئلة والاعتبارات الرئيسية

توجد الكثير من البيانات المحتملة، سواء في الصورة الكمية أو النوعية، التي يمكن استخدامها للتحقق من فاعلية الضمانات التسع للتخفيف من إساءة استخدام DNS. ومع ذلك، قبل تحديد البيانات المستخدمة، يجب تحديد تصميم للبحث لهيكلة البيانات وتحقيق أهداف المراجعة. ويجب أن يجيب أي تصميم للبحث على ما يلي:[84]

1. تحديد المشكلة البحثية بوضوح. ما هو اللغز التطبيقي الذي نحاول حله؟
2. مراجعة وتركيب المراجع المنشورة سابقًا المرتبطة بالمشكلة.
3. التحديد الواضح والصريح للأسئلة البحثية والافتراضات المرتبطة بالمشكلة البحثية.
4. البيان الفعال للبيانات اللازمة للإجابة المناسبة على أسئلة البحث و/أو اختبار الافتراضات وتوضيح كيفية الحصول على هذه البيانات.
5. بيان طرق التحليل المستخدمة على البيانات في تحديد ما إذا كانت الافتراضات صحيحة أم خاطئة.

توضح الأسئلة والأجوبة أدناه سياق هذه المهام البحثية من حيث مراجعة إساءة استخدام DNS:

1. تحديد المشكلة البحثية بوضوح. ما هو اللغز التطبيقي الذي نحاول حله؟

المشكلة البحثية: ليس واضحًا مدى فاعلية الضمانات للحد من إساءة استخدام DNS في نطاقات gTLD الجديدة.
اللغز التطبيقي: تشير بعض المؤشرات إلى انخفاض درجة إساءة استخدام DNS في نطاقات TLD بصورة عامة (القديمة والجديدة)، بينما تشير أخرى إلى زيادة المعدلات في نطاقات TLD محددة. يستمر عدم وضوح مدى فاعلية الضمانات في الحد من إساءة استخدام DNS في هذا التغيير.

2. مراجعة وتركيب المراجع المنشورة سابقًا المرتبطة بالمشكلة.

يقصد من هذا التقرير تقديم هذه المراجعة والتركيب.

3. التحديد الواضح والصريح للأسئلة البحثية والافتراضات المرتبطة بالمشكلة البحثية.

أسئلة البحث: بم تفسر التغيير في معدلات إساءة الاستخدام في مختلف نطاقات TLD؟ ما مدى فاعلية الضمانات المعمول بها لتلافيها؟

أمثلة الافتراضات (راجع النماذج أدناه لاستعراض تفصيلي لتحديد العلاقات الافتراضية):

- عالية المستوى (لتوجيه كامل المراجعة أو جزء كبير منها):
  - تسببت توسعة DNS في زيادة مقدار إساءة استخدام DNS التي تتناسب مع التوسعة نفسها.
- منخفضة المستوى (لتوجيه أجزاء محددة من الاستفسار في المراجعة):
  - كانت الضمانة "س" التي يقصد منها منع "ص" من إساءة استخدام DNS غير فاعلة في أهدافها المحددة

كما يجب أن توضح أسئلة البحث وافتراضاته أيضًا كيفية تعريف كل مصطلح وقياسه. على سبيل المثال، كما هو معروض أعلاه كيف يمكننا قياس فاعلية الضمانات؟

4. البيان الفعال للبيانات اللازمة للإجابة المناسبة على أسئلة البحث و/أو اختبار الافتراضات وتوضيح كيفية الحصول على هذه البيانات.

---

[84] تم اقتباس هذا من القائمة الموجزة للأسئلة البحثية في جامعة ساوذرن كاليفورنيا على http://libguides.usc.edu/writingguide/researchdesigns (بتاريخ 26 فبراير 2016).

على سبيل المثال، يمكن قياس فاعلية الضمانات من الناحية النوعية من خلال المقابلات مع الخبراء والمستخدمين للضمانات. كما يمكن قياس درجة مساهمة برنامج gTLD الجديد في إساءة استخدام DNS نوعيًا من خلال فحص العلاقات الإحصائية بين عدد النطاقات الجديدة ووكيل إساءة استخدام DNS مثل معدل التصيد.

5. بيان طرق التحليل المستخدمة على البيانات في تحديد ما إذا كانت الافتراضات صحيحة أم خاطئة.

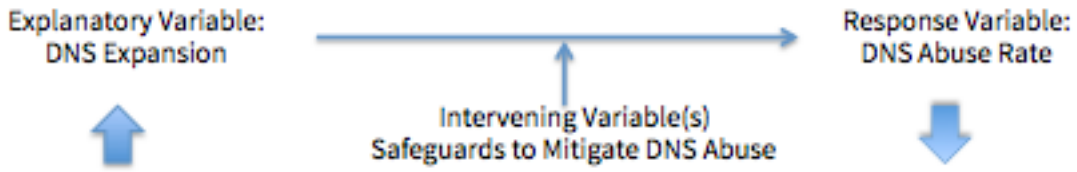
يتحدد وفقًا لأعمال CCT-RT، بالإضافة إلى تحديد أسئلة البحث وافتراضاته على النحو المعروض أعلاه.

النماذج والافتراضات العابرة

تم استنتاج النماذج أدناه من افتراضية مركزية بسيطة بأنه، من الناحية النظرية على الأقل، يجب أن يتسبب طرح الضمانات لمنع إساءة استخدام DNS في نطاقات gTLD الجديدة في مساحة DNS أنظف (أي توجد بها أنشطة ضارة أقل) مقارنة بفترة TLD القديم عند عدم وجود هذه الضمانات.

تم التوصل إلى ثلاثة سيناريوهات افتراضية قابلة للاختبار من هذا النموذج الأساسي:

النموذج 1: ترتب على توسعة DNS انخفاض نسبي في إساءة استخدام DNS (افتراضية الضمانة الفعالة)

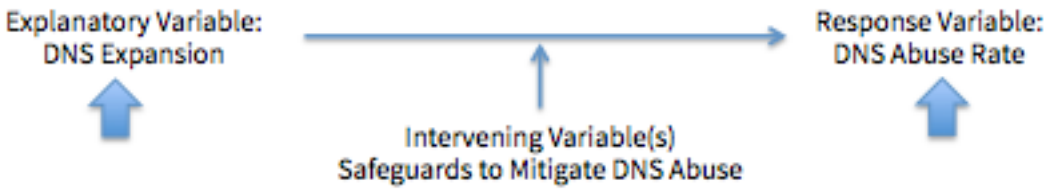


سؤال البحث: ما مدى توضيح العوامل العابرة للضمانات الفعالة للانخفاض النسبي في إساءة استخدام DNS؟

الافتراضية 1: تعتبر توسعة DNS المضمونة أحد العوامل العابرة التي توضح الانخفاض النسبي في إساءة استخدام DNS في نطاقات TLD الجديدة و/أو القديمة و/أو كامل DNS (تقسيم التحليل حسب الجديدة و/أو القديمة و/أو كامل DNS حسبما يكون مناسبًا).

الافتراضية 1.1: كانت الضمانات المفعلة للحد من إساءة استخدام DNS فعالة فيما يتعلق بتحقيق الأهداف المقصودة، وعوامل عابرة توضح الانخفاض النسبي في إساءة استخدام DNS (الضمانات الفردية المستهدفة للتحليل حسبما يكون مناسبًا).

النموذج 2: ترتب على توسعة DNS من خلال برنامج gTLD الجديد ارتفاع نسبي في إساءة استخدام DNS (افتراضية الضمانة غير الفعالة)

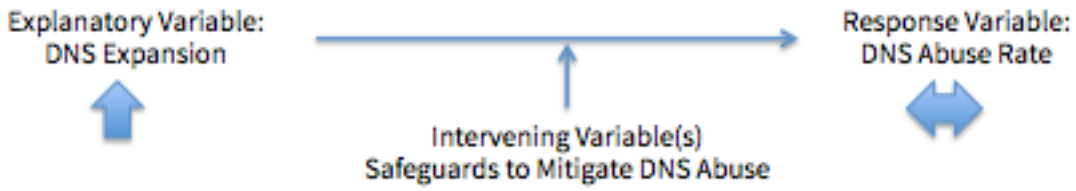


سؤال البحث: ما مدى توضيح العوامل العابرة للضمانات غير الفعالة للارتفاع النسبي في إساءة استخدام DNS؟

الافتراضية 2: تعتبر توسعة DNS المضمونة أحد العوامل العابرة التي توضح الارتفاع النسبي في إساءة استخدام DNS في نطاقات TLD الجديدة و/أو القديمة و/أو كامل DNS (تقسيم التحليل حسب الجديدة و/أو القديمة و/أو كامل DNS حسبما يكون مناسبًا).

الافتراضية 2.1: كانت الضمانات الموضوعة للحد من إساءة استخدام DNS غير فعالة فيما يتعلق بتحقيق الأهداف المقصودة (الضمانات الفردية المستهدفة للتحليل حسبما يكون مناسبًا).

النموذج 3: لم يكن لتوسعة DNS انخفاض تأثيرًا على إساءة استخدام DNS (افتراضية الضمانة غير الفعالة)



سؤال البحث: ما مدى توضيح العوامل العابرة للضمانات غير الفعالة لعدم التغير في إساءة استخدام DNS؟

الافتراضية 3: لم يكن لتوسعة DNS المضمونة تأثيرًا على نسبة إساءة استخدام DNS في نطاقات TLD الجديدة و/أو القديمة و/أو كامل DNS (تقسيم التحليل حسب الجديدة و/أو القديمة و/أو كامل DNS حسبما يكون مناسبًا).

الافتراضية 3.1: كانت الضمانات المفعلة للحد من إساءة استخدام DNS غير فعالة فيما يتعلق بتحقيق الأهداف المقصودة بتوفير مساحة gTLD أكثر أمانًا مقارنة بالمساحة القديمة (الضمانات الفردية المستهدفة للتحليل حسبما يكون مناسبًا).

إضافة إلى ذلك، بقدر ما تتعلق أعمال CCT-RT، يعرض هذا المقترح البحثي أسلوبًا محتملاً لهيكلة الاستفسار حول فاعلية الضمانات التسع للتخفيف من إساءة استخدام DNS. ويمكن أن يستدعي هذا الأسلوب توظيف بائعين خارجيين لديهم خبرة في تجميع وتحليل البيانات الإحصائية والنوعية بهدف إنشاء وتنفيذ الدراسة الفعلية. ولا يزال على فريق CCT-RT مهمة تحديد نطاق وطريق أي تحليل. كذلك، في حالة عدم وجود بديل، يعتبر مقترح البحث نقطة الخروج لمناقشة الأساليب الأخرى المحتملة.

الملحق: استبيان الأنشطة المرتبطة بإساءة الاستخدام في ICANN

المشروع	المجال	المصدر والروابط
اتفاقية السجل، المواصفة 11	البند 3أ: "يلتزم مشغل السجل بإدراج حكم في اتفاقية السجل-أمين السجل تشترط على أمناء السجلات إدراج أحكام اتفاقيات التسجيل الخاصة بهم تحظر على حاملي اسم المسجل من توزيع البرامج الضارة أو شبكات بوتنت التشغيلية الضارة أو رسائل التصيد أو القرصنة أو العلامات التجارية أو التعدي على حقوق المؤلف أو الممارسات الاحتيالية أو المضللة أو التزوير أو الانخراط في أنشطة خلاف ذلك تتعارض مع القوانين المعمول بها وتزويد (بما يتفق مع القوانين المعمول بها وأي إجراءات ذات صلة) عواقب لمثل هذه الأنشطة بما في ذلك تعليق اسم المجال". البند 3ب: "يلتزم مشغل السجل بإجراء تحليل فني دوري لتقييم ما إذا كانت النطاقات في نطاق TLD الخاص به يجري استخدامه في ارتكاب تهديدات للأمن أم لا، مثل السطو على مواقع الويب، والاحتيال، والبرامج الضارة، وشبكات بوتنت. كما يلتزم مشغل السجل بالحفاظ على تقارير إحصائية حول عدد تهديدات الأمان المحددة والإجراءات التي يتم اتخاذها نتيجة لفحوصات الأمن الدورية. ويلتزم مشغل السجل بالحفاظ على هذه التقارير طوال مدة هذه الاتفاقية ما لم يقتضي القانون فترة أقصر أو الموافقة عليها من جانب ICANN، وتقديمها إلى ICANN لدى طلبها."	المصدر: اتفاقية السجل الرابط: اتفاقيات السجل الرابط: الأسئلة المتكررة: المادة 11 من اتفاقية سجل gTLD الجديد المعدلة
توصية فريق مراجعة SSR رقم 11	التوصية 11: "يتعين على ICANN إنهاء وتنفيذ مقاييس نجاح نطاقات gTLD الجديدة وتعقب IDN السريع الذي يرتبط بوضوح بأهداف برنامجها ذات الصلة بـ SSR، بما في ذلك المقاييس الخاصة بفاعلية الآليات الخاصة بالحد من إساءة استخدام اسم النطاق."	المصدر: فريق مراجعة مرونة واستقرار وشفافية نظام أسماء النطاقات الرابط: تقرير فريق استعراض أمن واستقرار ومرونة DNS النهائي
نصيحة GAC: ICANN53 وICANN54	بيان بيونس آيريس الصادر عن ICANN53: "توصي GAC... أن يقوم مجتمع ICANN بوضع منهجية متسقة لتقييم عدد من أسماء النطاقات المسيئة ضمن الممارسة الحالية لتقييم برنامج gTLD الجديد." بيان دبلن الصادر عن ICANN54: "توصي GAC وتحث مجلس الإدارة على... وضع واعتماد منهجية متسقة لإبلاغ مجتمع ICANN بالمستويات واستمرار السلوك التعسفي (على سبيل المثال، البرمجيات الخبيثة، والروبوتات، والتصيد، والتزييف والقرصنة والعلامات التجارية و / أو التعدي على حق المؤلف والتزوير والممارسات الاحتيالية أو المضللة والسلوك غير القانوني) التي حدثت في بداية تنفيذ برنامج gTLD الجديد."	المصدر: اللجنة الاستشارية الحكومية في ICANN الرابط: بيان GAC الرسمي في بوينس آيرس لاجتماع ICANN53 الرابط: بيان GAC الرسمي في دبلن لاجتماع ICANN54
"استشارة SSAC حول حماية المسجل: أفضل الممارسات من أجل الحفاظ على الأمن والاستقرار في دورة حياة إدارة الاعتمادات	التوصية 1: كجزء من التقارير العادية، يتعين على إدارة الامتثال في ICANN نشر البيانات حول المخالفات الأمنية التي أبلغ أمناء السجل عنها وفقًا لاتفاقية اعتماد أمناء السجل لسنة 2013، البند 3.20." التوصية 2: "يجب إدراج حكم مماثل للوارد في اتفاقية اعتماد أمناء السجل لسنة 2013، البند 3.20 في كافة عقود السجل المستقبلية، مع نشر إحصاءات مماثلة وفقًا للتوصية 1 أعلاه."	المصدر: اللجنة الاستشارية للأمن والاستقرار الرابط: استشارة SAC074

مؤشر صحة سوق gTLD	وضعت ICANN مجموعة من مفاهيم المرشحين للنقاش المجتمعي للإعلام عن إنشاء مؤشر صحة سوق gTLD الذي يركز على (1) المنافسة القوية، (2) ثقة المستهلك (3) الاستقرار غير التقني. يقصد من هذه المفاهيم المقترحة تسهيل مناقشة المجتمع حول ما تعنيه "صحة سوق gTLD العالمي." كما كان منتظرًا من هذا النقاش المجتمعي أن يصدر عوامل قابلة للقياس لتعمل كمؤشرات الأداء الرئيسية لسوق gTLD. تركز بعض المفاهيم على إساءة استخدام DNS على النحو المبين.	المصدر: فريق عمل ICANN الرابط: مقترح مؤشر صحة السوق: الدعوة لإبداء التعليقات والمتطوعين