TLD-OPS

أمن واستقرار ccTLD معًا
التحذيرات الأمنية ● مستودع جهات اتصال الحوادث ● التعاون العالمي

إن TLD-OPS هو المجتمع الفني العالمي المعني بالرد على الحوادث لنطاقات ccTLD ومن خلالها. كما يقوم بتجميع كل من هو مسئول عن الأمن والاستقرار التشغيليين عن نطاقات ccTLD الخاصة بهم.

إن هدف مجتمع OPS-TLD يتمثل في تمكين مشغلي نطاقات ccTLD على مستوى العالم من اكتشاف والحد من الحوادث التي قد تؤثر على الامن والاستقرار التشغيليين لخدمات ccTLD للإنترنت الأوسع، مثل هجوم حجب الخدمة الموزعة DDoS، وحالات الإصابة بالبرامج الضارة وهجوم التصيّد. كما أن TLD-OPS متاح أمام جميع نطاقات ccTLD وتجمع الآن ما بين 340+ شخصًا مسئولون عن الأمن والاستقرار التشغيليين لعدد 188 نطاق ccTLD (بما يغطي 65%). كما يعمل TLD-OPS على مزيد من توسيع نطاق هياكل وعمليات وأدوات الرد والاستجابة على الحوادث الحالية للأعضاء ولا يستبدل أي منها.

سجل الاتصالات

ويعمل مجتمع OPS-TLD على بناء قائمة بريدية قياسية تعمل بمثابة مستودع لجهات اتصال الرد من أجل نطاقات ccTLD. حيث يتلقى المشاركون بريدًا إلكترونيًا يتم استخراجه تلقائيًا من القائمة مرة واحدة شهريًا ويحتوي على معلومات الرد على الحوادث لجميع أعضاء نطاقات ccTLD (جهات الاتصال وأرقام الهواتف وعناوين البريد الإلكتروني). وهذا من شأنه تحسين مستوى التواصل مع أعضاء TLD-OPS حيث يكون لدى الجميع معلومات الاتصال الخاصة بكل الآخرين متاحة بالفعل في صندوق الوارد، وهو ما يعمل بالتأكيد في حالات الطوارئ التي يكون فيها الاتصال مقطوعًا.

التحذيرات الأمنية

حيث تمثل TLD-OPS نسبة 65% من جميع نطاقات ccTLD على مستوى العالم، دائمًا ما يستخدم الأعضاء أيضًا القائمة البريدية من أجل مشاركة تنبيهات واستعلامات الأمان، على سبيل المثال في حالات هجوم حجب الخدمة الموزعة DDoS والبرامج الضارة التي تستخدم مساحة أسماء نطاقات ccTLD. وحيث إن الرد والاستجابة للحوادث تتعلق بالمعرفة والتعلم، فإننا نوصي الأعضاء بمشاركة ونشر طريقة تعاملهم مع بعض الحوادث، سواء على القائمة البريدية أو في ورشة عمل TLD-OPS السنوية (المتاحة مع كل "اجتماع أ") لهيئة ICANN.

الحوكمة

تم إعداد قائمة OPS-TLD بمعرفة نطاقات ccTLD ومن أجلها في الفترة 2015/2014 [1]. وهي خاضعة لإدارة مجتمع ccTLD بالكامل وذلك من خلال اللجنة الدائمة لقائمة TLD-OPS، والتي تتألف من المسئولين عن تشغيل نطاقات ccTLD التي تغطي جميع المناطق الجغرافية الخمسة (أفريقيا وآسيا-المحيط الهادئ وأوروبا وأمريكا الشمالية وأمريكا اللاتينية-الكاريبي) بالإضافة إلى ممثلين من SSAC وIANA وفريق أمن ICANN. وتشرف اللجنة الدائمة على التشغيل اليومي للقائمة والتطوير الإضافي "لمنظومة TLD-OPS". كما توفر ICANN الدعم الإدارة من خلال أمانة سر ccNSO. ويعمل

189
الأعضاء*

160 نطاق ccTLD بنظام ASCII
من .ad (أندورا) إلى .zm (زامبيا)

29 نطاقًا من نطاقات ccTLD ذات أسماء IDN
من .ভারত (الهند) إلى .المغرب (المغرب)

الأشخاص
340+ خبيرًا في مجال أمن واستقرار ccTLD التشغيليين

الحوكمة
100% من خلال نطاقات ccTLD، وذلك من خلال لجنة TLD-OPS الدائمة

القيمة المضافة
تحسين قدرة نطاق ccTLD الخاص بك على البحص في حالات الرد على الحوادث، واستلام ومشاركة تنبيهات واستعلامات الأمن ذات الصلة

*اعتبارًا من 2 يونيو، 2017.
قائمة الأعضاء الحاليين متوفرة على صفحة TLD-OPS الرئيسية.

الصفحة الرئيسية لمجتمع TLD-OPS
http://ccnso.icann.org/resources/tld-ops-secure-communication.htm

TLD-OPS

أمن واستقرار ccTLD معًا
التحذيرات الأمنية ● مستودع جهات اتصال الحوادث ● التعاون العالمي

خادم القائمة على "أرضية محايدة" في مركز عمليات وتحليل وأبحاث DNS أو DNS-OARC.

الاشتراك سهل!

يعد الاشتراك في قائمة TLD-OPS سهلاً للغاية نظرًا لأنها قائمة بريدية. وعلى الرغم من ذلك لا يمكن الوصول إلى القائمة إلا من خلال الأشخاص المسئولين عن الأمن والاستقرار التشغيليين لنطاق ccTLD ومن تم تفويضهم على هذا النحو من خلال جهة الاتصال الإدارية الخاصة بهم في IANA.

وللاشتراك في القائمة، اطلب من جهة الاتصال الإدارية الخاصة بك في IANA إرسال بريد إلكترون بالأسماء وعناوين البريد الإلكتروني وأرقام الهواتف الخاصة بجهات الاتصال المعنية بالأمن والاستقرار لنطاق ccTLD الخاص بك إلى أمانة سر ccNSO. برجاء استخدام نموذج الاشتراك إلى اليمين، والمتوفر كذلك للنسخ واللصق على صفحة TLD-OPS الرئيسية.

هام: يجب أن يأتي بريدك الإلكتروني الخاص بطلب الاشتراك من عنوان جهة الاتصال الإدارية التي سجلت بها في الوقت الحالي في قاعدة بيانات IANA [2]. فإذا لم يكن ذلك ممكنًا، فيجب عليك نسخ عنوان البريد الإلكتروني هذا في البريد الإلكتروني الخاص بطلب الاشتراك. وإلا، فلن نتمكن من إضافتك إلى القائمة.

الثقة الشخصية

تستند قائمة TLD-OPS إلى الثقة الشخصية، وهو ما يعني أن بإمكان المشاركين المشاركة باستخدام بريدهم الإلكتروني الخاص وأرقام هواتفهم. ويتمثل الهدف الكامن وراء ذلك في أن نموذج الثقة الشخصية سوف يسهم في إرساء مزيد من الثقة داخل مجتمع ccTLD، على سبيل المثال لأن الناس يبدأون في التعرف على أسماء بعضهم البعض والتقوا بعضهم البعض في ورش عمل TLD-OPS. ومن غير المسموح استخدام عناوين بريد إلكترونية رغم ذلك تكون مستندة إلى الدور أو الوظيفة على القائمة.

علمًا بأن نموذج الاستشهاد المستخدم بشكل عام في مجتمع الرد على الحواد غير مناسب لعمليات TLD-OPS نظرًا لأن مجتمع ccTLD عبارة عن مجموعة كبيرة (291 نطاق ccTLD على الإجمال) لدرجة أنه سوف يكون من الصعب ضم أشخاص غير معروفين نسبيًا على القائمة باستخدام هذا النموذج.

نموذج الاشتراك

برجاء استخدام التنسيق التالي للاشتراك في قائمة TLD-OPS. كما أنه متوفر كذلك من صفحة TLD-OPS الرئيسية للنسخ واللصق.

-- بداية الرسالة --
من: جهة اتصال مدير IANA في نطاق ccTLD أو المفوض المرخص له
إلى: أمانة سر ccNSO <ccnsosecretariat@icann.org>
نسخة إلى: عنوان جهة اتصال مدير IANA في نطاق ccTLD
الموضوع: طلب الاشتراك في قائمة TLD-OPS البريدية

السادة؛ أمانة ccNSO،

أود تقديم طلب لاشتراك الأشخاص التالية أسماؤهم في قائمة TLD-OPS. وأؤكد بموجب هذا الخطاب على مسئوليتهم عن الأمن والاستقرار الإجماليين لنطاق ccTLD الخاص بي، وأنني جهة اتصال مدير IANA لنطاق ccTLD الخاص بي أو أنني مرخص للتصرف بالنيابة عن/عنها.

مع أطيب التحيات،

جهة اتصال مدير <ccTLD>

== INCIDENT RESPONSE CONTACT INFORMATION ==

Contact Person #1 (primary):
الاسم: <FirstName1> <LastName1>
عنوان البريد الإلكتروني: <EmailAddress1>
رقم الهاتف المحمول: +<country code> <number>

Contact Person #2 (secondary):
الاسم: <FirstName2> <LastName2>
عنوان البريد الإلكتروني: <EmailAddress2>
رقم الهاتف المحمول: +<country code> <number>

Contact Person #3:
الاسم: <FirstName3> <LastName3>
عنوان البريد الإلكتروني: <EmailAddress3>
رقم الهاتف المحمول: +<country code> <number>
-- نهاية الرسالة --

قواعد الانخراط بالعمل

تُعامل جميع المعلومات التي يتم تبادلها على القائمة للحصول على معلومات اتصال الاستجابة للحوادث في أي نطاق ccTLD معاملة سرية ولا يجوز مشاركتها خارج مجتمع TLD-OPS.

كما يجب تمييز المعلومات الخاصة بحوادث الأمن الفعلية وذلك من خلال استخدام ألوان بروتوكول إشارات مرور البيانات (TLP) [2]: أحمر (معلومات موجهة لمستلمين محددين فقط)، أصفر (توزيع محدود)، أو أخضر (توزيع على مستوى المجتمع)، أو أبيض (توزيع غير محدود). ويتبع مجتمع TLD-OPS تعريفات TLP لـ US-CERT [3] واللون الافتراضي هو TLP-AMBER.

لا يجب على أعضاء القائمة مشاركة المعلومات المستخرجة تلقائيًا على القائمة. فقائمة TLD-OPS غير مشفرة من أجل تمكين جميع نطاقات ccTLD من المشاركة. ■

المصادر

[1] التقرير النهائي لمجموعة عمل SECIR، http://ccnso.icann.org/workinggroups/secir.htm

[2] قاعدة بيانات جذر IANA، https://www.iana.org/domains/root/db

[3] بروتوكول إشارات مرور البيانات، http://en.wikipedia.org/wiki/Traffic_Light_Protocol

[4] تعريف US-CERT لمصطلح TLP، https://www.us-cert.gov/tlp

نبذة عن

نشرة من إعداد لجنة TLD-OPS الدائمة.
الإصدار 2.5،
في 12 يونيو 2017.