ورقة تقنية · إطار عمل مقترح · الإصدار 1.0

من الكشف إلى تنفيذ تدابير الاستجابة

بنية قابلة للقياس للاستجابة لـ DNS Abuse: مصدر الأدلة وسلسلة حيازتها، والإجراء المتناسب، والمساءلة العامة، والاستئناف السريع—صُممت للاختبار لا لمجرد الادعاء.

نُشر في 2 أغسطس 2026 · PhishDestroy البحوث · مسودة للاستشارة العامة · لم يخضع للمراجعة من قبل الأقران

PD-WP-2026-01 · الإصدار 1.0 · نُشر في 2 أغسطس 2026
الرابط الدائم: https://phishdestroy.io/ar/dns-abuse-enforcement-framework

الملخص

اقتراح مستقل · ليس برنامجًا تابعًا لـ «ICANN»

استنتاج مباشر. يحتوي النظام التعاقدي الخاص بـ«gTLD» على فجوة قابلة للقياس بين الاستخدام الخبيث لنطاق ما — الذي تم التحقق منه تقنيًّا — والتدابير الفعالة للتخفيف من آثاره. تُظهر الدراسات المنشورة أن العديد من حملات التصيد الاحتيالي تستمر لساعات أو أيام، في حين أن إجراءات الامتثال التعاقدي قد تستغرق عدة أيام عمل. ويوضح نموذج السيناريو المكشوف كيف يؤدي التأخير إلى زيادة العائدات المتوقعة للحملة؛ وبُعد النطاق الذي يتراوح بين 60 و85% التقدير الرئيسي القابل للاختبار الوارد في الورقة البحثية للضرر الذي يترتب على الإشعار، وليس إحصائية ثابتة لجميع حالات الاحتيال العالمية. يتعلق التقدير الهندسي الذي يتراوح بين 100 و150 دولارًا بجمع ومعالجة المراجعة الأولية لمجموعة محددة من بيانات المنطقة وشفافية الشهادات والتغذية العامة، وليس بالتكلفة الكاملة للمراجعة القانونية أو الإنفاذ. تقترح الورقة الأدلة الموقعة، وأهداف الاستجابة القابلة للقياس، والتصعيد التلقائي للحالات التي تم التحقق من صحتها، والتدابير التصحيحية المتناسبة، والمساءلة العامة، والاستئناف السريع. ولا تقترح منح المبلغين وصولاً مباشرًا إلى أدوات التحكم في تعليق النطاقات.

- **المصدر الأساسي** — مدعوم بشكل مباشر بوثيقة رسمية أو دراسة منشورة.
- **نموذج توضيحي** — حساب قابل للتكرار تستند مدخلاته إلى افتراضات، وليس إلى متوسطات السوق.
- **مقترح سياساتي** — تصميم معروض للتشاور والاختبار والمراجعة.

01 السؤال البحثي، ونطاق البحث، ومعيار الإثبات

السؤال أضيق نطاقًا من «من الذي فشل؟»: **ما هي حالات التأخير الملحوظة بين الأدلة المؤكدة واتخاذ الإجراءات المتناسبة التي يمكن تجنبها، وما هو التدخل الذي يقلل من الضرر الذي يلحق بالضحية دون التسبب في حالات إيجابية كاذبة غير مقبولة أو أضرار جانبية؟**

يشمل نطاق الدراسة النظام البيئي التعاقدي لـ gTLD: المسجلون، والموزعون، ومسجلو النطاقات، وسجلات النطاقات، ووحدة الامتثال التعاقدي التابعة لـ ICANN. ولا يتم تضمين مزودي خدمات الاستضافة، وشبكات توزيع المحتوى (CDNs)، والمتصفحات، وخدمات الدفع، ومنصات الإعلان، وفرق الاستجابة للطوارئ الحاسوبية (CERTs) الوطنية، وسلطات العدالة الجنائية إلا في الحالات التي تؤثر فيها على سلسلة الأدلة أو سلسلة الاستجابة. تخضع نطاقات المستوى الأعلى ذات رموز البلدان (country-code TLDs) لنظام حوكمة مختلف، ولا يُفترض أنها خاضعة لعقود ICANN الخاصة بـ gTLD.

حالة الأطروحات الرئيسية

- تحلل هذه الورقة موقع «ICANN» باعتباره مؤسسة خاصة معنية بالحوكمة والالتزام التعاقدي ضمن منظومة «gTLD». ولا يُعد موقع «ICANN» هيئة تنظيمية حكومية أو جهة معنية بإنفاذ القانون، لكنه يقوم باعتماد مسجلي النطاقات، وإبرام العقود مع مشغلي السجلات، وإنفاذ تلك الاتفاقيات؛ ولا يُعفي هذا النطاق المحدود من المسؤولية المؤسسية.
- يُعد النطاق الذي يتراوح بين 60 و85% تقديرًا كميًّا أساسيًّا في نموذج الضرر الذي تتناوله الورقة البحثية. ويُقدَّم هذا التقدير باعتباره تقديرًا قابلاً للاختبار مستمدًّا من افتراضات صريحة وملاحظات على حالات محددة — وليس كإحصائية ثابتة مسبقًا تشمل جميع حالات الاحتيال على مستوى العالم. وتتمثل الخطوة التالية في مجال الأدلة في نشر مجموعة بيانات على مستوى الحوادث تربط بين الطوابع الزمنية الخاصة بالكشف والإبلاغ والتخفيف والضرر.
- يُعد الرقم الذي يتراوح بين 100 و150 دولارًا تقديرًا هندسيًّا قابلًا للاختبار للميزانية اللازمة للجمع المستمر والفرز الأولي لمجموعة محددة من بيانات «المنطقة القابلة للوصول» و«شفافية الشهادات» و«التغذية العامة» المتعلقة بالبنية التحتية للسلع الأساسية. وهو لا يمثل تكلفة الرؤية العالمية الكاملة، أو المراجعة القانونية، أو الطعون، أو التوافر العالي، أو الإنفاذ. لذلك، تتعامل الورقة مع هذا الرقم كمعيار مرجعي يمكن تكراره باستخدام حمل عمل منشور وقائمة جرد للمصادر وسجل للتكاليف — وليس كسعر عالمي تم إثباته بالفعل. ويضيق هذا التمييز نطاق الادعاء دون محو التباين في التكاليف الذي يجري اختباره.
- تتناول المقارنة التي أجرتها الدراسة على مدى ثلاثة أسابيع «زمن الاستجابة للامتثال»، وليس اتفاقية مستوى الخدمة (SLA) الشاملة لإزالة المواقع. موقع «ICANN» الأسئلة الشائعة حول الامتثال التعاقدي تنص على أن معظم أنواع الشكاوى يمكن أن تمر بثلاث فترات رد متتالية مدة كل منها خمسة أيام عمل قبل إحالتها رسميًا إلى مستوى أعلى، في حين أن العديد من الحملات الخبيثة تستمر لساعات أو أيام. وتقتضي العقود بشكل منفصل اتخاذ إجراءات تخفيفية فورية ومناسبة فور توفر أدلة قابلة للتنفيذ. [2] [4]
- في حالة وجود تسجيل خبيث تم التحقق منه ومخصص لغرض واحد، `serverHold` تُعد هذه الإجراء من أكثر الإجراءات تسببًا في الاضطرابات على مستوى نظام أسماء النطاقات (DNS)، لأنها تزيل التفويض من المنطقة. وهي ليست شاملة: فقد تؤدي أيضًا إلى تعطيل خدمة البريد الإلكتروني والنطاقات الفرعية والخدمات المشروعة؛ وقد تظل الإجابات المخزنة مؤقتًا سارية حتى انتهاء صلاحية TTL؛ وقد تتطلب الخدمات المخترقة أو المشتركة إجراءات تخفيف أضيق نطاقًا. [4] [7]

> **المساهمة البحثية**
>
> هذا الاقتراح قابل للتفنيد. يمكن للباحث أن يقارن بين المجموعات التجريبية والمجموعات الضابطة من حيث «الوقت المستغرق حتى التقييم الأولي»، و«الوقت المستغرق حتى التخفيف»، ومؤشرات الخسائر بين الضحايا، ومعدل التكرار، والنتائج الإيجابية الكاذبة، و«وقت التراجع»، والتأثيرات الجانبية.

02

ما تثبته المصادر الأولية

$165.1M

ICANN FY27 تمويل العمليات

تم اعتماد ميزانية «FY27». مقياس سياقي؛ وليس الإنفاق وفقًا لـ «DNS Abuse». [1]

191,561

2025 شكوى تتعلق بالتصيد الاحتيالي/انتحال الهوية في عام 2025

أكبر فئة شكاوى لدى IC3 من حيث العدد؛ خسائر مخصصة مباشرة بقيمة 215.8 مليون دولار. [10]

24 ساعة

متوسط العمر في إحدى الدراسات التي أجريت عام 2021

نتيجة خاصة بمجموعة البيانات تشمل 1,288 نطاقًا للتصيد الاحتيالي؛ وليست مدة صلاحية عامة. [11]

لا توجد اتفاقية مستوى الخدمة (SLA) محددة

الموعد النهائي العام لإزالة المحتوى

تستخدم تعديلات عام 2024 مصطلحي «الفورية» و«المناسبة» في سياق تدابير التخفيف، بدلاً من تحديد موعد نهائي شامل واحد. [2] [3]

الاقتراح	الحالة	ما يمكن قوله
التصيد الاحتيالي هو DNS Abuse	تم التحقق منه	التصيد الاحتيالي واحد صراحةً من الفئات الخمس التي تشملها التعديلات التعاقدية الخاصة بـ gTLD لعام 2024. [2]
يجب على جهات التسجيل أن تتصرف	تم التحقق منه	يجب على جهات التسجيل أن تتصرف سريعًا عندما تكون لديها أدلة قابلة للتنفيذ على أن اسمًا ترعاه يُستخدم في DNS Abuse. [2]
يجب على مشغلي السجلات أن يتصرفوا	تم التحقق منه	يجب على مشغلي السجلات أن يتصرفوا سريعًا عندما يقررون بصورة معقولة، استنادًا إلى أدلة قابلة للتنفيذ، أن اسمًا مسجلًا يُستخدم في DNS Abuse؛ ويظل التدبير المناسب معتمدًا على السياق. [3]
`serverHold` يلغي التفويض	تم التحقق منه	إنها حالة "EPP" التي يحددها الخادم. وقد تظل الإجابات المخزنة مؤقتًا في ذاكرة التخزين المؤقتة DNS سارية حتى انتهاء صلاحيتها، ويؤثر هذا الإجراء على النطاق المسجل بأكمله. [7]
يمكن رؤية جميع حالات DNS Abuse في CZDS أو CT	خطأ	تمثل CZDS وCertificate Transparency مستشعرين مفيدين، لكنهما لا يقدمان رؤية كاملة أو آنية لجميع استخدامات النطاقات. [8] [9]

سجل التقرير نصف السنوي الأول الصادر عن شركة ICANN بشأن تنفيذ المتطلبات التعاقدية بموجب تعديلات عام 2024، 192 تحقيقًا، وأكثر من 2,700 نطاق مُعلَّق، وأكثر من 350 صفحة تصيد تم تعطيلها، وإخطارين بحدوث خرق. لا تثبت هذه الأرقام أن الضوابط الحالية كافية، لكنها تستبعد الادعاء المطلق بأن النظام لا يتخذ أي إجراء. [5]

03 لماذا لا يزال زمن استجابة الشبكة هدفًا بحثيًا مشروعًا

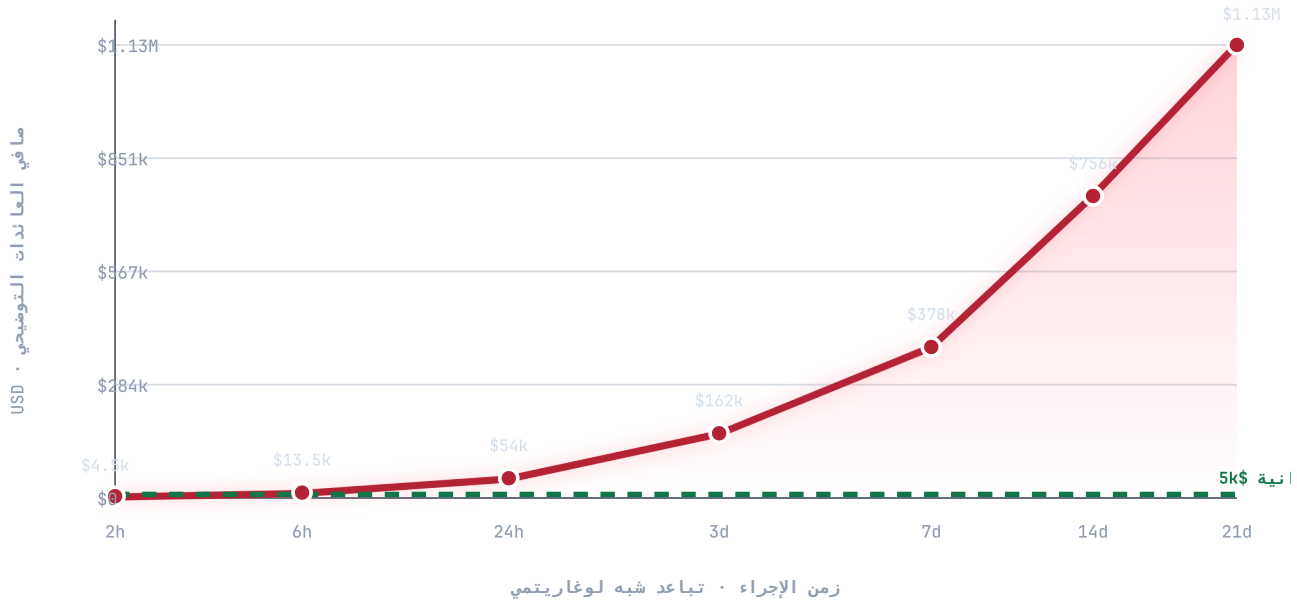
تستمر بعض عمليات التصيد الاحتيالي لفترات تتراوح بين ساعات وأيام. وقد أشار بيجمانز وزملاؤه في دراسة أُجريت عام 2021 إلى أن متوسط العمر الافتراضي الملحوظ لـ 1,288 نطاقًا من نطاقات التصيد الاحتيالي بلغ 45 ساعة، بينما بلغ الوسيط 24 ساعة. [11] أفادت دراسة أجريت عام 2026 حول نطاقات التصيد الاحتيالي المسجلة حديثًا بوجود توزيع شديد الانحراف: فمن بين 14,112 نطاقًا يمكن قياس مدة بقائها، بلغ المتوسط 8.6 أيام، والوسيط يومًا واحدًا. [12] لا يمكن تعميم أي من هذين المثالين على جميع فئات التهديدات، لكن كلاهما يوضح لماذا قد تفوت العملية التي تُقاس بالأيام العملية فقط عمليات الاحتيال والتصيد الاحتيالي قصيرة الأمد.

التباين الزمني المقاس

لا تحدد هذه الدراسات حجم الضرر المالي الذي يحدث بعد الإخطار، لكنها تثبت وجود تباين زمني: فالعملية التي قد تستغرق مراحل الامتثال غير الرسمية المبكرة فيها ما يصل إلى خمسة عشر يوم عمل لا يمكن أن تشكل بحد ذاتها استجابة للحوادث في الحملات التي يبلغ متوسط مدة استمرارها حوالي يوم واحد. وبالتالي، فإن نقطة الـ 21 يومًا المذكورة أدناه تمثل سيناريوًّا لـ «تأخر الامتثال»، وليست تسميةً لاتفاقية مستوى الخدمة (SLA) عالميةً تحت عنوان «ICANN».

الشكل 1 · النتيجة التراكمية التوضيحية لعملية الاحتيال والتصيد الاحتيالي

النموذج · التباعد الزمني الشبيه بالسجل



يُظهر هذا المنحنى السيناريو الوارد في القسم 4؛ وهو ليس بيانات سوقية ملاحظة. وقد تم تقليص الفترات الطويلة في المنحنى أفقياً لتسهيل قراءته. المصدر: نموذج قابل للتكرار مع مدخلات معلنة.

الحذر السببي

إن تقصير مدة بقاء النطاق لا يعني تلقائيًّا تجنب الخسائر المالية. فقد ينتقل المهاجمون إلى مواقع أخرى، أو يستخدمون مواقع تم اختراقها، أو يغيرون قنوات التوزيع، أو يسحبون الأموال قبل اكتشافهم. لذا، يجب قياس الأثر السببي، لا استنتاجه من سرعة إزالة الموقع وحدها.

04 اقتصاديات عملية الاحتيال والتصيد بوصفها سيناريو قابلًا لإعادة الإنتاج

غالبًا ما لا يكون الأصل ذو الأهمية الاقتصادية هو رسوم التسجيل، بل حركة المرور والمحتوى الإبداعي والبنية التحتية والثقة المتراكمة حول النطاق. وهذه الفكرة تبدو معقولة؛ إلا أن حجمها يختلف باختلاف عمليات الاحتيال والتصيد. ولذلك، فإن الآلة الحاسبة أدناه تكشف عن كل المدخلات بدلاً من تقديم نتيجة افتراضية على أنها متوسط ملاحظ.

تعريف النموذج

$$\begin{aligned} \text{visits}(T) &= \text{daily\_traffic} \times T / 24 \\ \text{victims}(T) &= \text{visits}(T) \times \text{conversion\_rate} \\ \text{proceeds}(T) &= \text{victims}(T) \times \text{average\_loss} \times (1 - \text{cashout\_attrition}) \\ \text{profit}(T) &= \text{proceeds}(T) - \text{campaign\_budget} \end{aligned}$$

حاسبة السيناريوهات

قم بتغيير أي افتراض. القيم الواردة هي لأغراض التوضيح فقط ولا تمثل تقديرات لسوق التصيد الاحتيالي النموذجي.

نموذج توضيحي

ميزانية عملية الاحتيال والتصيد (USD)

5000

الزيارات اليومية

2000

نسبة تحويل الضحايا (%)

1.5

متوسط الخسارة لكل ضحية (USD)

2400

فاقد تسييل العائدات (%)

25

الزمن حتى الإجراء (بالساعات)

24

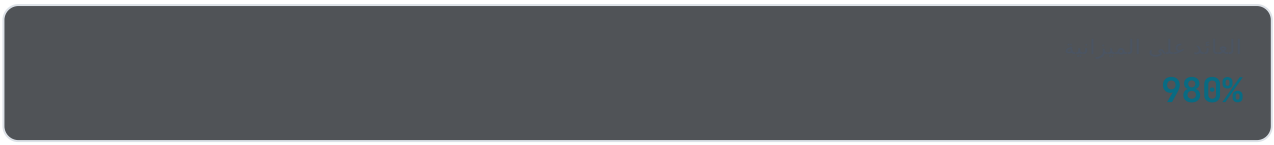
2,000

30

$54,000

$49,000

h 2.2



قد يكون العدد المتوقع للضحايا كسريًّا لأن النموذج يعبّر عن قيمة متوقعة. ولا يأخذ في الحسبان تراجع حركة الزيارات، أو تغيّر السلوك بعد الكشف، أو انتقال الحملة إلى بنية أخرى، أو تكرار الضحايا، أو توزيعات عدم اليقين.

◄ عرض جدول مصدر النموذج

05 قياس الضرر الذي يمكن تجنبه دون التظاهر بالدقة

لا يمكن أن تصبح «الخسارة بعد الكشف» نتيجة مفيدة إلا إذا تم تعريف «الكشف» و«التسليم» و«الضرر» بشكل متسق. ولا يُعد الطابع الزمني للقائمة السوداء دليلاً على أن المسجل قد تلقى أدلة قابلة للتنفيذ. كما أن معاملة المحفظة لا تُعزى تلقائيًا إلى نطاق واحد. ولا يُحدد عدم إمكانية الوصول إلى نطاق ما الجهة الفاعلة التي تسببت في هذا التغيير.

الحد الأدنى لمخطط الحدث

الحدث	الطابع الزمني المطلوب	الحد الأدنى من الإثبات
الملاحظة الأولى	`t_obs`	المستشعر، تجزئة الطلب/الاستجابة، طريقة الالتقاط، مصدر الساعة.
التحقق الفني	`t_valid`	المؤشر القابل للتكرار، وهوية المراجع، وفئة التهديد، ودرجة الثقة.
تم تسليم الإشعار	`t_notice`	نسخة من إيصال التسليم المُصدق ومجموعة المستندات الإثباتية.
يقر الطرف المسؤول بما يلي:	`t_ack`	رقم تعريف الحالة والدور المستهدف: المضيف، أو المسجل، أو السجل، أو المنصة، أو السلطة.
لوحظ حدوث تخفيف	`t_التخفيف`	DNS، وHTTP، وحالة الدفع أو حالة المنصة، يتم قياسها من زوايا رؤية متعددة.
الاستئناف / الاستعادة	`t_restore`	أساس القرار، وتغير الأدلة، والتحقق من الاستعادة.
حدث الضرر	`t_harm`	تقرير عن الضحية بعد إزالة العناصر المُعرِّفة، أو معاملة يمكن ربطها بالضحية، أو أي دليل بديل موثق آخر.

مقياس النتائج المقترح

```
= Post-notice harm share
attributable harm with t_harm > t_notice
──────────────────────────────────────
all attributable harm in the observation window
```

يجب أن يستخدم البسط والمقام نفس قاعدة الإسناد. وينبغي أن تتضمن النتائج بيانات عن المجموعة، وفترة الثقة، والرقابة اليمنى، والمصادر المفقودة، ومعالجة حالات تكرار الضحايا، والحساسية تجاه نافذة الملاحظة. وينبغي حصر

استخدام مصطلح «قابل للوقاية» في التصميم السببي أو، على الأقل، في المقارنة المتطابقة — وليس في كل حدث يحدث بعد الإخطار.

التقدير النموذجي المركزي · 60–85%

تحتفظ الورقة بنسبة تتراوح بين 60 و85 في المائة كتقدير أساسي لحصة الضرر المنسوب الذي يحدث بعد الكشف والإخطار في فئة الحوادث قيد النمذجة. وهذا تقدير سيناريو مستمد من الافتراضات المعلنة وملاحظات الحالات — وليس إحصائية مقاسة لجميع حالات الاحتيال على مستوى العالم. وينبغي استخدامه في تحليل الحساسية إلى أن تتوافق مجموعة البيانات على مستوى الحوادث مع الملاحظات والأدلة التي تم التحقق من صحتها، بالإضافة إلى توقيتات التنفيذ والتخفيف والضرر. ويُعد نشر تلك المجموعة من البيانات هو الاختبار الإثباتي لهذه الفرضية، وليس سببًا لحذفها.

06 الخريطة المؤسسية: القدرات موزعة

لا يوجد طرف واحد يرى أو يتحكم في الحادثة برمتها. فالمسجل على علم بالعلاقة بين المسجل والمستجل؛ والسجل يتحكم في حالة النطاق التي يحددها السجل؛ والمضيف وCDN يتحكمان في توصيل المحتوى؛ والمتصفحات ومزودي خدمات الأمان يتحكمون في التحذيرات؛ ومزودي خدمات الدفع والمحافظ الإلكترونية يمكنهم إيقاف التحويلات؛ والسلطات يمكنها فرض الحفظ أو المصادرة. يقوم موقع ICANN بصياغة العقود وإنفاذها في النظام البيئي gTLD، لكنه لا يدير مستوى تحكم عالمي EPP.

01 · الإشارة

الباحثون وأجهزة الاستشعار

رصد مؤشرات المحتوى والبنية التحتية والضحايا؛ وحفظ مصدر الأدلة وسلسلة حيازتها.

02 · الخدمات

المضيف / CDN / المنصة

يمكن إزالة المحتوى أو الوصول إليه بسرعة، وغالبًا دون تغيير النطاق.

03 · الراعي

جهة التسجيل

تقوم بمراجعة الاستخدامات التقنية الضارة، وتتواصل مع صاحب التسجيل، ويمكنها تعيين الحالة من جانب العميل.

04 · المنطقة

مشغل السجل

يتحكم في حالة مجموعة السجلات EPP وتفويض منطقة TLD.

05 · العقد

ICANN الامتثال

تتحقق من امتثال الأطراف المتعاقدة؛ ولا تنظر في كل قضية احتيال.

06 · القانون

CERT / السلطات

تنسيق الاستجابة واستخدام الصلاحيات القانونية الخاصة بكل ولاية قضائية.

لا تعني القدرة الموزعة انعدام المسؤولية. فلا يتخلص المسجل الراعي من واجباته التعاقدية بتفويض معالجة حالات إساءة الاستخدام إلى موزع؛ حيث يتحكم السجل في حالة EPP المحددة على الخادم؛ وتقوم منظمة «ICANN» بفرض الامتثال التعاقدي. يجب أن يسجل سجل التدقيق ليس فقط من قام بالتصرف، بل ومن تلقى أدلة قابلة للمتابعة، ومن أعاد توجيه القضية، ومن لم يرد، أو من لم يؤدِ واجباً موكلاً إليه. تظل السلطة القانونية في يد الجهة المخولة بتطبيق الإجراء؛ وتشمل المساءلة أيضاً حالات عدم الأداء الموثقة.

تركيز التمويل وفرضية قابلة للاختبار بشأن تضارب الحوافز

$165.1M

تمويل عمليات «ICANN» للسنة المالية 27

تم اعتماد الميزانية الأساسية للسنة المالية 27. [1]

≈98.1%

مصادر إيرادات السجل ومسجل الأسماء

ما يقارب 162.0 مليون دولار من خطة التمويل البالغة 165.1 مليون دولار. [1]

70.7%

الرسوم المستندة إلى المعاملات وحدها

$116.8M tied to billable domain transactions. [1]

وبالتالي، فإن هيكل التمويل يتركز بشكل كبير على المدفوعات الواردة من الأطراف المتعاقدة التي تنفذ «ICANN» الاتفاقات المبرمة معها، كما أن حصة كبيرة منه تتأثر بمعاملات التسجيل القابلة للفوترة. وهذا يخلق تبعية هيكلية ويثير مسألة مشروعة تتعلق بتضارب الحوافز. وهو ما لا، في حد ذاتها، لا تثبت وجود تقصير متعمد في إنفاذ القوانين أو حدوث «استيلاء تنظيمي» كامل. وينبغي اختبار فرضية «الاستيلاء التنظيمي» في ضوء أوقات الاستجابة على مستوى كل حالة على حدة، ونتائج الإنفاذ، والعقوبات، وتكرار الانتهاكات، ودور الأطراف المعنية التي تتلقى التمويل في قرارات السياسة العامة والتنفيذ.

07 الخط الأساسي التعاقدي لعام 2024 — وما لم يحدده

أنشأت التعديلات العالمية التي أُدخلت في أبريل 2024 على اتفاقية اعتماد جهات التسجيل واتفاقية السجل الأساسية التزامات صريحة بالتخفيف من DNS Abuse. يجب على جهات التسجيل أن تتصرف سريعًا عندما تكون لديها أدلة قابلة للتنفيذ على أن اسمًا ترعاه يُستخدم في DNS Abuse. ويجب على مشغلي السجلات أن يتصرفوا سريعًا عندما يقررون بصورة معقولة، استنادًا إلى أدلة قابلة للتنفيذ، أن اسمًا مسجلًا يُستخدم في DNS Abuse. وفي الحالتين يعتمد التدبير المناسب على السياق والخطورة والأضرار الجانبية. [2] [3]

ثلاثة خطوط زمنية غالبًا ما يتم الخلط بينها

الجدول الزمني	ما الذي ينطبق عليه	ما لا يعنيه ذلك
24 ساعة	مراجعة التقارير المستندة إلى أسس سليمة بشأن نشاط غير قانوني، والمقدمة إلى جهة الاتصال المخصصة بموجب RAA §3.18.3 من سلطات إنفاذ القانون أو حماية المستهلك أو الجهات شبه الحكومية أو الجهات المماثلة.	وهذا ليس موعدًا نهائيًا عامًّا لتعليق النطاق خلال 24 ساعة.
"على الفور"	اتخاذ تدابير التخفيف المناسبة بعد استيفاء عتبة الأدلة القابلة للتنفيذ المعمول بها.	فليس هناك عدد محدد من الساعات، ولا يتطلب الأمر نفس الإجراء في كل حالة.
21 يومًا	يمكن أن تُعتبر فترة تصحيح بعد إصدار إشعار رسمي بالخرق بموجب العقد.	فهذا ليس العمر الافتراضي المعتاد الذي يُمنح لكل نطاق ضار يتم الإبلاغ عنه.

لهذه المرونة مزاياها: فلا ينبغي التعامل مع نطاق جامعي تعرض للاختراق كما لو كان نطاقًا للتصيد الاحتيالي مسجَّلًا حديثًا ومخصصًا لغرض واحد. وتكمن مشكلة المساءلة في صعوبة المقارنة بين مصطلحي «فوري» و«مناسب» في غياب الطوابع الزمنية المنشورة وفئات الحالات ورموز النتائج. ويضيف الاقتراح الوارد أدناه آليات للقياس والمراجعة دون الادعاء بأن موعدًا نهائيًّا واحدًا يناسب كل الحالات.

08 مشكلة الحدود: يتم تغطية عمليات التصيد الاحتيالي؛ لكن بعض حالات الاحتيال المالي قد لا يتم تغطيتها

يندرج التصيد الاحتيالي صراحةً ضمن التعريف التعاقدي لـ DNS Abuse. وتكمن الحدود الأصعب في المواقع التي تخدع المستخدمين باسم أصلي بدل انتحال طرف ثالث محدد، مثل بعض منصات الاستثمار المزيفة والمتاجر الاحتيالية وعمليات احتيال استرداد الأموال ومخططات توقيع المحافظ. وبحسب الوقائع، قد تُعامل هذه الحالات بوصفها إساءة على مستوى محتوى الموقع أو احتيالًا على المستهلك أو فئة قانونية أخرى، لا DNS Abuse تعاقديًا.

تسمية البحث المقترحة

الإساءة الموثقة المسببة لضرر مالي (VFHA): استخدام موثق لنطاق بهدف الحصول بالخداع على أموال أو بيانات دفع أو مفاتيح خاصة أو عبارات استرداد، بصرف النظر عن انتحال العلامة التجارية. ولا يُعد VFHA من مصطلحات ICANN الحالية، ولا ينشئ بذاته سلطة تعاقدية.

يمكن للمشاورات السياساتية أن تبحث ما إذا كانت فئة ضيقة قائمة على الأدلة مثل VFHA ينبغي أن تُدرج في العقود المستقبلية أو إطار إحالة عابر للقطاعات أو القانون الوطني. ويجب أن يتطلب التوسع اختبارًا دقيقًا للضرر، وأدلة موثوقة، وسبل انتصاف متناسبة، ومراجعة للاختصاص، واستثنافًا. ولا تكفي تسمية «احتيال» مبهمة.

09 ما يجب أن تثبته الادعاءات المتعلقة بخدمات المراقبة التي تتراوح تكلفتها بين 100 و150 دولارًا شهريًّا — وما لا يمكنها إثباته

يمكن لخادم عادي تنزيل لقطات متاحة لملفات مناطق gTLD المشاركة وحساب التغييرات محليًّا، واستيعاب أحداث «شفافية الشهادات» (Certificate Transparency) المحددة والتغذيات المفتوحة، وتوحيد السلاسل النصية، وحساب التجزئات، وتحديد أولويات المرشحين. وهذا معيار هندسي مفيد وقابل للاختبار — وليس «مراقبة كاملة للإنترنت». في الربع الثاني من عام 2026، أبلغت شركة Verisign عن 401.6 مليون تسجيل عبر جميع نطاقات المستوى الأعلى (TLDs)؛ وتغطي CZDS ملفات منطقة gTLD المشاركة بدلاً من جميع نطاقات المستوى الأعلى، بينما تسجل CT الشهادات أو الشهادات المسبقة المسجلة علنًا بدلاً من كل نطاق نشط أو ضار. [8] [9] [17]

القدرة	نموذج أولي اعتيادي	خدمة للصالح العام على مستوى الإنتاج
استيعاب المنطقة/CT/الموجزات	ممكن لمجموعة مصادر محددة	مجمّعات احتياطية، وعقود مصادر، ومراقبة الفجوات
فرز السلاسل/التجزئات	ممكن	قياس معياري، وكشف الانحراف، ودراسات السلبيات الكاذبة
عرض المتصفح	مجموعة فرعية صغيرة بالعينة	بيئة تنفيذ معزولة، ونقاط رصد إقليمية، واحتواء البرمجيات الخبيثة
تحديد قانوني	غير مشمول	مراجعون مؤهلون، ورسم خريطة الاختصاص والسلطة
توافر عالٍ / حفظ الأدلة	غالبًا غير متاح	توقيعات مدعومة بـ HSM، وسجلات تدقيق، ونسخ احتياطية، واستجابة للحوادث
الاستئناف والاستعادة	غير مشمول	تشغيل 24/7، وتصعيد مستقل، وأهداف خدمة

الشكل 2 · سياق ترتيب الأوامر — العرض اللوغاريتمي · التكاليف غير المتماثلة

تساعد العرض اللوغاريتمي على إبقاء القيم الصغيرة مرئية. الأرقام الثلاثة الأولى هي افتراضات هندسية أو برمجية معلنة تتطلب معيارًا مرجعيًّا منشورًا، وليست عروض أسعار من الموردين. ICANN تمويل العمليات هو رقم مُثبت على نطاق مؤسسي. هذه ميزانيات غير متكافئة عن قصد: تهدف المقارنة إلى اختبار ما إذا كانت عمليات الجمع والفرز الأساسية تمثل تكلفة باهظة بطبيعتها، وليس ما إذا كان برنامج الإنفاذ الكامل يكلف 100 دولار شهريًّا.

10 إطار الاستجابة المقترح لحالات DNS Abuse المتحقق منها

الإطار المقترح هو بنية مرجعية، وليس «مفتاح إيقاف عالمي» تلقائي. فهو يعمل على توحيد متطلبات الملف وسجل القرار والطوابع الزمنية، مع السماح للمشغل المصرح له باختيار الإجراء الفعال الأقل إزعاجًا.

01 · الاستيعاب

الحصول عليها وحفظها

جمع التقارير والملاحظات؛ تحليل البيانات الأولية؛ مزامنة الساعات.

02 · مصدر الأدلة وسلسلة حيازتها

توحيد الأدلة

تسجيل المنشأ والطريقة وسجل المعالجة والتبعيات من المصادر.

03 · التحقق من الصحة

تأكيد

قم بتكرار السلوك الضار وتمييز الأدلة المستقلة.

04 · التقييم

المخاطر والضمانات

صنف حالات التسجيل الضار، والخدمات المخترقة، والاستضافة المشتركة، ودرجة خطورتها.

05 · الرد

الإبلاغ والتخفيف من الآثار

تحديد الجهة المسؤولة، والموعد المستهدف، والحل الفعال الأقل إزعاجًا.

06 · مراجعة

التدقيق والاستئناف

نشر البيانات الوصفية للنتائج، وقياس الأثر، ودعم التصحيح السريع.

مستويات الأدلة

E1

إشارة غير مؤكدة

معلومات من مصدر واحد، أو تطابق لغوي، أو ادعاء يتعلق بالسمعة. مناسبة للمراقبة، ولا تكفي أبدًا بمفردها لاتخاذ إجراء التعليق.

E2

السلوك الذي تم تكراره

لقطة موثقة بختم زمني تُظهر سرقة بيانات الاعتماد، أو توزيع برامج ضارة، أو مسار معاملة خادع.

E3

التحقق المستقل

مصدران مستقلان حقًّا على الأقل، أو دليل تقني قابل للتكرار، بالإضافة إلى التحقق من الملكية والسياق.

E4

التأكيد المؤهل

الجهة المختصة، والخدمة المتضررة، ومالك العلامة التجارية، أو أدلة الضحية التي تم التحقق من صحتها، مع سلسلة حيازة تضمن حماية الخصوصية.

قاعدة الاستقلال

تُعد ثلاثة موجزات تنسخ قائمة الحظر نفسها من المصدر الأعلى مصدرًا واحدًا، لا ثلاثة. ويجب أن يوضح مخطط مصدر الأدلة وسلسلة حيازتها الأصل المشترك والمزامنة وإعادة النشر من جانب المورّد.

11 حزمة أدلة دنيا وواجهة API قابلة للتشغيل البيني

يجب أن يقوم نظام الإبلاغ عن التهديدات (API) بإنشاء حالة قابلة للتحقق وبدء مؤقت استجابة قابل للتدقيق؛ ويجب ألا يتمكن المبلغ من إصدار أمر تعليق مباشرةً. إذا كانت حالة E3/E4 تتعلق بتسجيل ضار ذي غرض واحد وانتهت صلاحيتها دون صدور قرار مسبب أو اتخاذ إجراءات تخفيف فعالة، فإن النظام يقوم تلقائيًّا بتصعيدها إلى مشغل السجل أو جهة أخرى تتمتع بسلطة تعاقدية أو قانونية. أ `serverHold` لا يمكن أن يصدر الأمر إلا من جهة مخولة. ويُعتبر كل من «التصعيد التلقائي» و«سلطة السجل للتصرف عند انتهاء الصلاحية» تغييرات مقترحة في السياسة، وليست ادعاءات بشأن سلطة قائمة. ويتم توقيع كل انتقال بين الحالات وإرفاقه بسجل التدقيق.

مثال · POST /v1/cases

```
}
,indicator": {"type": "domain", "value": "example.invalid"}"
,"alleged_category": "credential_phishing"
,"observed_at": "2026-08-02T06:14:22Z"
] :"evidence"
}
,"type": "http_capture"
,"…sha256": "a3f1c9"
,"collection_method": "isolated_browser_v2"
"…source_id": "reporter:ed25519:7c2a"
{
,[
,"…provenance_graph": "ipfs-or-object-store:sha256:91bd"
} :"collateral_context"
,registered_domain_scope": true"
,shared_service": false"
,mail_observed": true"
suspected_compromise": false"
,{
,"requested_action": "review"
"…:reporter_signature": "ed25519"
{
```

تُرجع الاستجابة الناجحة معرّف القضية، والجهة المستلمة، ومستوى الأدلة، وأخطاء الاكتمال، والوقت المستهدف للمراجعة، وعنوان URL العام الخاص بالشفافية. ويجب ألا تتعهد بتدبير تصحيحي محدد قبل أن تقوم الجهة المختصة بتقييم الصلاحيات والتأثيرات الجانبية.

12 أهداف الاستجابة المقترحة، وليس مواعيد نهائية عامة لإزالة المحتوى

ينبغي الفصل بين أهداف مستوى الخدمة *شكر وتقدير*, *الفرز*, *القرار* و *التخفيف الفعال*. وهذا يجعل الأداء قابلاً للقياس دون افتراض أن التعليق هو النتيجة الصحيحة دائماً.

ملخص القضية	الإقرار	هدف الفرز	هدف القرار	خيارات الرد النموذجية
سرقة بيانات اعتماد الدفع من نوع E3/E4 أو عبارة البذرة في عملية تسجيل خبيثة مخصصة لغرض واحد	15 دقيقة	1 ساعة	4 ساعات	كتلة المحتوى؛ تعليق التسجيل/السجل عند الاقتضاء؛ تحذيرات المتصفح والدفع.
عمليات التصيد الاحتيالي التي تستهدف العلامة التجارية E3 أو توزيع البرامج الضارة	30 دقيقة	2 ساعة	6 ساعات	إزالة المضيف/CDN، أو اتخاذ إجراءات التخفيف على مستوى النطاق، أو توجيه حركة المرور إلى «حفرة امتصاص» (sinkhole)، أو إصدار تحذير وفقًا لنقطة التحكم.
نطاق شرعي تم اختراقه أو مستأجر SaaS مشترك	1 ساعة	4 ساعات	12 ساعة	عزل المسار/الحساب واستعادة المالك؛ تجنب تعليق النطاق المسجل حيثما أمكن ذلك.
الاحتيال المالي مع تصنيف موضع نزاع	4 ساعات	12 ساعة	24 ساعة	الحفظ، والتدخل على مستوى المنصة/الدفع، والإحالة إلى الجهة المختصة، والقرار المسبب.
إشارة E1 أو تقرير غير مكتمل	تلقائي	24 ساعة	لا شيء حتى يتم التحقق من صحتها	مراقبة الأدلة وإثرائها وطلبها.

هذه أهداف تجريبية. وينبغي استنباط القيم الصحيحة استنادًا إلى مدة بقاء التهديدات الملحوظة، ومستوى التوظيف، وتكلفة الأخطاء، والقيود القانونية، ثم نشرها مع توزيعات معدلات تحقيق الأهداف بدلاً من متوسط واحد.

13 السلامة، والإجراءات القانونية السليمة، والخصوصية، وأنماط الفشل

قد يؤدي الاستجابة السريعة دون اتخاذ تدابير وقائية إلى تفاقم مشكلة البيانات الخاطئة، مما قد يتسبب في الرقابة أو التخريب التجاري أو انقطاع خدمات البنية التحتية. ولذلك، فإن البنية التحتية السليمة تعامل «النتائج الإيجابية الخاطئة» و«الأضرار الجانبية» على أنها إخفاقات أمنية من الدرجة الأولى.

نمط الفشل	عنصر التحكم المطلوب	مقياس قابل للتدقيق
بلاغ كاذب ضد أحد المنافسين	التحقق من صحة المراسل، وسمعة المصدر، وإعادة الإنتاج المستقلة، والعقوبات المفروضة على الاستخدام التقني الضار	معدل التقارير المرفوضة حسب المُبلغ؛ حالات التلاعب المؤكدة
دورة التغذية التي تتنكر في صورة إجماع	مخطط مصدر الأدلة وإزالة تكرار المصادر العليا	عدد المصادر المستقلة قبل تصحيح السلالة وبعده
تم تعليق جميع النطاقات الشرعية المخترقة بشكل جماعي	تصنيف نية التسجيل وتفضيلات التخفيف على مستوى المسار	نسبة النطاقات المخترقة؛ الخدمات الشرعية المتأثرة
تسربت بيانات الضحايا أو تفاصيل الثغرة الأمنية إلى العلن	الإفصاح المتدرج، وحجب المعلومات، والأدلة المختومة، وحدود الاحتفاظ	حوادث انتهاك الخصوصية؛ نتائج مراجعة عمليات حجب المعلومات
استمرار الممارسات غير المشروعة	استقبال الاستئناف 24/7، ومراجع مستقل، ومسار استعادة موثّق	الوسيط ووقت الانعكاس في المئوية 95
توقف السجل يتسبب في انقطاع خدمة البريد الإلكتروني/النطاقات الفرعية	قائمة الضمانات، وتناسب التدابير التصحيحية، والرصد اللاحق للإجراءات	الخدمات التي تعرضت للتعطيل لكل إجراء؛ معدل الرجوع إلى الحالة السابقة

الضمانات الدنيا للإجراءات القانونية السليمة

1. يتم تسجيل رمز السبب، ومستوى الدليل، وصانع القرار المسؤول عن كل إجراء تقييدي.
2. يمكن للمسجل الحصول على بيان بالأسباب يراعي الخصوصية وتقديم أدلة مضادة.
3. تتم مراجعة الحالات العاجلة استئناف من قبل شخص لم يشارك في اتخاذ القرار الأصلي.
4. ينتشر التراجع عبر نفس القناة ذات الإشارة التي استخدمت في الإجراء الأصلي.
5. إحصاءات الأخطاء والاستعادة الإجمالية متاحة للجمهور؛ أما الأدلة الحساسة فتظل خاضعة لضوابط الوصول.

14

من «مؤشر السمية» إلى «مؤشر جودة الاستجابة» القابل للمساءلة

يمكن أن تسهم درجة المسجل العامة في تعزيز المساءلة، لكن التصنيفات السطحية تتأثر بشكل مشوه بحجم المحفظة، ونطاق التغطية، وتركيبة العملاء، وما إذا كانت النطاقات قد سُجلت بنية خبيثة أو تعرضت للاختراق لاحقًا. ولا يجب أبدًا أن تُستخدم الدرجة كمبرر للحظر الجماعي لجميع عملاء المسجل.

متجه الجودة المقترح

```
:RQI = report as a vector, not a single opaque rank

                coverage-adjusted validated-abuse rate
        median / p90 acknowledge, triage and decision times
                mitigation effectiveness and recurrence
                    false-positive and reversal rates
                  median / p95 appeal-resolution time
            evidence completeness and transparency rate

,Always publish N, observation window, confidence intervals
.feed coverage and malicious-registration / compromise split
```

إذا كان من الضروري استخدام مؤشر مركب لأغراض الحوكمة، فيجب تحديد الأوزان قبل التقييم، وإجراء اختبارات الحساسية واختبارات الأداء الرجعي على الحالات التي تم استبعادها. وينبغي تصنيف النتائج حسب نوعية التسجيل (TLD)، وحجم المسجل، وفئة التهديد، ومصدر الدليل. وتكون النتيجة عبارة عن إشارة للمساءلة — وليست حكماً آلياً بشأن النطاق.

15 قاعدة بيانات عامة متدرجة الوصول لشفافية DNS Abuse

يمكن لسجل الشفافية أن يضع حداً للنزاعات حول ما إذا كان الإشعار موجوداً أم لا، ومتى تم تسليمه، وما هي الإجراءات التي تلت ذلك. غير أن نشر كل دليل قد يؤدي إلى الكشف عن هوية الضحايا، والبيانات الشخصية، وأساليب التحقيق، ومسارات الاستغلال الحالية. والحل يكمن في تطبيق نظام الوصول المتدرج.

P السجل العام

رقم القضية، والمؤشر، والفئة العامة، والطوابع الزمنية الرئيسية، ومستوى الأدلة، وأدوار الأطراف المعنية، ورمز النتيجة، وحالة «استئناف»، والتجزئات الخاصة بالأدلة المختومة.

C عرض معلومات الطرف المتعاقد

الأدلة الفنية القابلة للتكرار، وقناة الاتصال، والسياق المصاحب، وتعليمات الحفظ.

R عرض الصلاحيات المقيدة

بيانات الضحايا، وتحديد المسؤولية المالية، ومواد التحقيق الجاري، وسلسلة الحفظ غير المحجوبة.

كل تحديث يكون «لإضافة فقط»، ومُؤرخًا ومُوقَّعًا. ولا تؤدي التصحيحات إلى محو السجل السابق، بل تُضيف سجلًا جديدًا يحل محله. وينبغي أن يلتزم البحث العام بقواعد الاحتفاظ بالبيانات، ويمنع الكشف الجماعي عن هوية الضحايا، ويوفر سبل الانتصاف في حالة وجود بيانات شخصية غير دقيقة.

16

مشروع تجريبي مدته ستة أشهر مع تقييم مسبقًا

يجب أن يكون المشروع التجريبي المفيد صغيرًا بما يكفي لإدارته وكبيرًا بما يكفي لاختبار سلسلة السببية. النطاق المقترح: ثلاثة مسجلين متطوعين، واثنين من مشغلي السجلات، وشريك واحد في الاستضافة/CDN، ومصدرين مستقلين للبيانات البحثية، ولجنة مؤهلة من استئناف. يجب تسجيل بروتوكول الدراسة وتعريفات النتائج قبل توزيع الحالات.

الشهر 1

البروتوكول ورسم الخرائط القانونية

تحديد الفئات، والسلطات، ومستويات الأدلة، وتقييم الأثر على الخصوصية، وشروط الإيقاف.

الشهر 2

تطبيق الإجراءات الحالية

قياس الطوابع الزمنية والنتائج الأساسية دون تغيير سلوك الاستجابة.

الشهر 3

تشغيل حزمة الأدلة

إدخال مصدر أدلة موقّع، وإزالة التكرار، وتصنيف الأثر الجانبي.

الشهر 4

أهداف استجابة الاختبار

قم بتوزيع الحالات المؤهلة عشوائياً أو استخدم نهج التنفيذ التدريجي؛ وقم بمراقبة الأخطاء يومياً.

الشهر 5

ممارسة "استئناف" وحالات الفشل

إجراء تدريبات على استعادة البيانات، وإعداد تقارير خبيثة من «الفريق الأحمر»، ومراجعة ضوابط الوصول.

الشهر 6

التقييم المستقل

ينبغي نشر أحجام التأثيرات، وفترات الثقة، وحالات البيانات المفقودة، والأحداث السلبية، والتكاليف، والمواد اللازمة لتكرار الدراسة.

النتائج الأساسية للبرنامج التجريبي

- الزمن الوسيط وزمن المئين 90 من الأدلة المتحقق منها إلى التخفيف الفعّال.
- الفرق في الضرر المنسوب بعد الإخطار أو مؤشر بديل محدد مسبقًا لتعرض الضحية.
- معدل النتائج الإيجابية الكاذبة، ودرجة خطورة الإجراءات الخاطئة، والوقت المتوسط للاستعادة.
- التكرار على مستوى صاحب التسجيل نفسه ومجموعة البنية التحتية وعملية الاحتيال/التصيد.
- التكلفة التشغيلية المباشرة لكل حالة تم التحقق منها ولكل إجراء تخفيف فعال.

> قاعدة اتخاذ القرار
>
> لا تقم بالتوسيع إلا إذا أظهر البرنامج التجريبي فعالية أكبر بكثير في التخفيف من المخاطر، دون تجاوز الحدود المسجلة مسبقًا فيما يتعلق بحالات الإيجابية الكاذبة، وحوادث انتهاك الخصوصية، والتأخير في خدمة «استئناف»، أو الاضطرابات الجانبية في الخدمة.

17 الاستنتاجات والتوصيات القابلة للاختبار

ليست الاستجابة لحالات DNS Abuse مرشحًا تقنيًّا بحتًا، ولا مشكلة تستطيع مؤسسة واحدة حلها منفردة. فقد أرست تعديلات العقود لعام 2024 التزامات فعلية بالتخفيف، مع إبقاء مساحة واسعة للتقدير في الأدلة والتوقيت وسبل الانتصاف. وهذه السلطة التقديرية لازمة للتناسب، لكنها تجعل تقييم الأداء صعبًا في غياب سجلات قابلة للمقارنة.

1. **توحيد حزمة الأدلة.** اعتماد حقول موحدة لمصدر الأدلة والطوابع الزمنية والنتائج لدى المبلّغين وجهات التسجيل ومشغلي السجلات ومزودي البنية التحتية.
2. **قِس كل مرحلة على حدة.** انشر أزمنة تأكيد الاستلام والفرز واتخاذ القرار والتخفيف والاستئناف بحسب فئة التهديد ومستوى الدليل.
3. **التمييز بين التسجيل الخبيث والاختراق.** يُفضل اتباع مسار معالجة المشكلات أو إصلاح الحسابات فيما يتعلق بالخدمات الشرعية التي تعرضت للاختراق، والاحتفاظ بالتدابير التي تشمل النطاق بأكمله للحالات التي تكون فيها هذه التدابير متناسبة.
4. **اختبر أهداف الاستجابة تجريبيًّا.** اختبر أهدافًا زمنية بالساعات للتسجيلات الخبيثة عالية الثقة وأحادية الغرض، بدلًا من إعلان مهلة عامة.
5. **نشر بيانات المساءلة التي تراعي الخصوصية.** استخدم سجل شفافية متدرج يتضمن سجلات موقعة وأدلة مقيدة.
6. **قيّم الأثر السببي.** لا تساوِ بين تسريع التعليق وتوفير الأموال قبل أن تقيس دراسة مسجلة مسبقًا أثره على الضحايا وانتقال التهديد إلى قنوات أخرى.

والاستنتاج البناء هنا ليس أن المشكلة الأصلية تختفي بمجرد تقييد نطاق ادعاءاتها، بل أن الادعاءات الرئيسية أصبحت الآن قابلة للاختبار: فنطاق الضرر بعد الكشف الذي يتراوح بين 60 و85% يمثل فرضية كمية صريحة؛ و$100–150 يمثل افتراضًا هندسيًّا قابلًا للاختبار للميزانية الخاصة بطبقة محددة من أجهزة الاستشعار والفرز؛ ويمكن تجربة أهداف الاستجابة على نطاق الساعة بالنسبة للتسجيلات الخبيثة ذات الثقة العالية والغرض الواحد. ينبغي نشر حجم العمل والتكاليف والطوابع الزمنية والنتائج، ومقارنتها بخط أساس، وقياس الانحراف والخطأ. ومن شأن التأكيد أن يبرر التغيير التعاقدي والسياسي؛ أما الرفض فسيحدد الافتراض الذي فشل.

إفصاح عن التحرير والمنهجية. PhishDestroy هو مشروع مستقل وغير تجاري متخصص في استخبارات التهديدات. هذا المنشور هو اقتراح سياسي وهندسي، وليس مشورة قانونية، ولا برنامجًا تابعًا لمبادرة «ICANN»، ولا ورقة بحثية خضعت لمراجعة الأقران. أما نطاقات الميزانية المُصنَّفة على أنها «نماذج» فهي افتراضات تخطيطية. توجد روابط أدناه للمصادر الأولية التي استندت إليها الادعاءات. يمكن تقديم التصحيحات عبر قنوات الاتصال والإبلاغ المسؤول المتوفرة على الموقع.

موقف «الناظر من منظور الشخص الأول» · يجب أن تقيّد المساءلة كلاً من التقاعس والتجاوز

حدود شخصية لسلطة الإنفاذ

أنا لا أطلب — ولا أرغب — في الحصول على وصول مباشر إلى أداة حجب النطاقات. وتتطلب هذه الصلاحية مراجعة مستقلة، وسجلات تدقيق عامة، وإمكانية الاستئناف السريع، وإمكانية التراجع عن القرار.

أعتقد أن هناك العديد من الشركات المتميزة والمسؤولة التي يمكن الوثوق بها لتولي أجزاء من هذا العمل. وبناءً على خبرتي والسجل الذي نشرته، فإنني لا أدرج شركة «NameSilo» ضمن تلك المجموعة.

لا أنصح الشركات الأمريكية الشرعية بأن تعهد بمهام حساسة تتعلق بالإبلاغ عن الانتهاكات أو الأمن إلى متعاقدين معينين لا يمكن أن تصمد تضاربات مصالحهم أو كفاءتهم أو سلوكهم أمام التدقيق المستقل. فالأمر يتعلق بالأفعال الموثقة، وليس بالجنسية: فالأصل الروسي في حد ذاته لا يثبت شيئًا، تمامًا كما أن عنوان شركة أمريكية لا يثبت شيئًا.

أريد العدالة والمساءلة الحقيقية بالنسبة لمسجلي النطاقات الذين حققوا إيرادات من تسجيل وتجديد نطاقات تم توثيقها كجزء من حملات احتيال متكررة. وحيثما تشير الأدلة إلى ما يتجاوز مجرد الإهمال إلى احتمال التسهيل المتعمد —سواء كان ذلك من خلال المشاركة التشغيلية المباشرة أو العمل كوسيط مطلع كانت مهمته الحفاظ على تسجيل نطاق ضار وإبقائه متاحًا على الإنترنت على الرغم من التحذيرات المتكررة— فيجب إجراء تحقيق مستقل في هذا السلوك، وينبغي أن يترتب عليه عواقب إذا ثبتت صحته. لا أقدم الشكوك على أنها حقائق ثابتة؛ لكن صفة الوسيط يجب ألا تمنح حصانة من التدقيق.

مراجعة التحقيق الأساسي ↗

المراجع والملاحظات المتعلقة بالمصادر

[1] **ICANN, Adopted FY27 Budget (2026)** · https://www.icann.org/en/system/files/files/adopted-icann-budget-fy2027-published-2026-en.pdf

مصدر تمويل العمليات في FY27 البالغ 165.1 مليون دولار، وتكوين تدفقات التمويل.

[2] **ICANN, 2024 Global Amendment to the Registrar Accreditation Agreement** · https://www.icann.org/en/system/files/files/registrar-accreditation-agreement-global-amendment-05apr24-en.pdf

المصدر التعاقدي الأساسي لالتزامات جهات التسجيل بشأن DNS Abuse.

[3] **ICANN, 2024 Global Amendment to the Base gTLD Registry Agreement** · https://itp.cdn.icann.org/en/files/registry-agreements/base-registry-agreement-global-amendment-05-04-2024-en.html

المصدر التعاقدي الأساسي لواجبات التخفيف لدى مشغلي السجلات.

[4] **ICANN Contractual Compliance, DNS Abuse Obligations Advisory (2024)** · https://www.icann.org/en/contracted-parties/advisories/documents/advisory-compliance-with-dns-abuse-obligations-in-the-registrar-accreditation-agreement-and-the-registry-agreement-05-02-2024-en
التفسير التشغيلي، ومتطلبات البلاغات، وأمثلة على التخفيف المناسب.

[5] **ICANN, Enforcement of DNS Abuse Mitigation Requirements (2024)** · https://www.icann.org/en/system/files/files/icann-enforcement-of-dns-abuse-mitigation-requirements-08nov24-en.pdf
تقرير تنفيذ لمدة ستة أشهر، وأعداد التحقيقات وإجراءات التخفيف.

[6] **ICANN SSAC, SAC115: Report on an Interoperable Approach to Addressing Abuse Handling (2021)** · https://www.icann.org/en/system/files/files/sac-115-en.pdf
خلفية عن قابلية التشغيل البيني لبلاغات DNS Abuse وجودة الأدلة.

[7] **Hollenbeck, RFC 5731: EPP Domain Name Mapping (2009)** · https://www.rfc-editor.org/rfc/rfc5731.html
التعريف الفني لقيم حالة نطاق EPP، بما في ذلك الحالة التي يحددها الخادم.

[8] **Laurie et al., RFC 9162: Certificate Transparency Version 2.0 (2021)** · https://www.rfc-editor.org/rfc/rfc9162.html
المواصفات القياسية المعتمدة والحدود الخاصة بـ «CT» باعتباره جهاز استشعار.

[9] **ICANN, Centralized Zone Data Service** · https://www.icann.org/en/contracted-parties/registry-operators/services/centralized-zone-data-service
نطاق ونموذج الوصول لملفات مناطق «gTLD» المشاركة.

[10] **FBI Internet Crime Complaint Center, 2025 IC3 Annual Report** · https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
أرقام الشكاوى والخسائر المبلغ عنها، بما في ذلك عدد حالات التصيد الاحتيالي/انتحال الهوية.

[11] **Bijmans et al., Catching Phishers By Their Bait (USENIX Security, 2021)** · https://www.usenix.org/system/files/sec21-bijmans.pdf
قياسات خاصة بمجموعات البيانات المتعلقة بالبنية التحتية لعمليات التصيد الاحتيالي وفترات بقائها الملحوظة.

[12] **Newly Registered Domains and Phishing Lifetimes, Journal of Cybersecurity (2026)** · https://doi.org/10.1093/cybsec/tyag020
أدلة تجريبية حديثة حول نطاقات التصيد الاحتيالي المسجلة حديثًا وتوزيعها على مدار عمرها.

[13] **Inferential Analysis of Maliciously Registered Domains — INFERMAL (2024)** · https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf
ICANN - تحليل ممول يتعلق بالتسجيلات الخبيثة وعوامل النظام البيئي؛ والقيود ذات الصلة على الادعاءات السببية.

[14] **Chainalysis, 2026 Crypto Scam Trends** · https://www.chainalysis.com/blog/crypto-scams-2026/
تقدير أحد المزودين لتدفقات عمليات الاحتيال عبر السلسلة لعام 2025؛ لا يُعتبر ضمن إجمالي عمليات التصيد عبر النطاقات.

[15] **APWG, Phishing Activity Trends Report, Q1 2026** · https://docs.apwg.org/reports/apwg_trends_report_q1_2026.pdf
هجمات التصيد الاحتيالي/عناوين URL التي تم رصدها؛ ولا تعادل هذه المقاييس عدد النطاقات المسجلة الفريدة.

[16] **Cybercrime Information Center / Interisle, Phishing Landscape 2025** · https://www.cybercrimeinfocenter.org/phishing-activity-numbers-may-april-2025
يفصل بين الهجمات الملحوظة، والنطاقات الفريدة، والنطاقات المسجلة لأغراض خبيثة.

[17] **Verisign, Domain Name Industry Brief, Q2 2026** · https://blog.verisign.com/domain-names/q2-2026-domain-name-industry-brief-quarterly-report/
المصدر الذي استند إليه الرقم المُعلن عنه البالغ 401.6 مليون تسجيل عبر جميع نطاقات المستوى الأعلى (TLDs).