تقرير قُطري • QATAR 2026 · BRANDEFENSE COUNTRY REPORT · TLP:CLEAR • 79 دقيقة للقراءة

Brandefense: تقرير مشهد التهديدات السيبرانية في قطر 2026

انكشاف الهويات وادعاءات البيانات وموجة من نشاط الهاكتفيست في مركز متصل للطاقة والطيران

TRANSLATED WITH AI

ترجمت هذه النسخة بمساعدة الذكاء الاصطناعي من النسخة الإنجليزية الأصلية، وتعد النسخة الإنجليزية هي المرجع.

إعداد	نُشر	مدة القراءة
Odin by Brandefense	21 نوفمبر 2026	79 دقيقة للقراءة

النسخة	فترة البحث
الإصدار 1.0 · TLP:CLEAR · Public Research Edition	1 يناير–20 نوفمبر 2026

73 of 250
مؤسسة كان لديها بيانات اعتماد مدرجة للبيع يوم الفحص

7,867–8,175
منشورًا منقّحًا تبقى من أصل 55,241 منشورًا موسومًا

31,836
هجمات DDoS على قطر رصدتها NETSCOUT في الفترة يناير–يونيو 2026

9 of 9
المصارف المُصدِرة للبطاقات في قائمتنا التي لديها إدراج حالي لبيانات اعتماد، وهو أول بند يجب فرزه

المحتويات

01	الملخص التنفيذي		خريطة التقرير
02	السياق الرقمي والاستراتيجي لقطر	03	الانكشاف الوطني: 250 مؤسسة رائدة
04	ما نراه على الويب المظلم	05	أمثلة على الاستهداف بحسب القطاع
06	نشاط القرصنة الناشطة (الهاكتفيزم) وهجمات DDoS	07	الجهات الفاعلة في التهديد
08	اقتصاد الاحتيال	09	تحليل معمّق للقطاع المصرفي والمالي
10	الاستجابة التنظيمية والوطنية	11	التوقعات
12	خطة العمل	A	الملحق A. المنهجية

B الملحق B. سجل الأدلة

C الملحق C. المصادر

D الملحق D. مسرد المصطلحات

عن هذا التقرير

الفصل 1

الملخص التنفيذي

يجيب هذا الفصل عن

ماذا حدث في 2026، وما الأهم بالنسبة إلى المؤسسات القطرية، وما الذي ينبغي أن يقرره القادة أولًا؟

4

قرارات للقادة، كل منها مرتبط بأدلة في فصول التقرير

في هذا الفصل

أربعة قرارات للقادة
العام بالأرقام

باختصار

بالنسبة إلى المؤسسات الـ 250 المختارة، بنطاق رئيسي واحد لكل منها (68 منها مرتبطة مبدئيًا)، يتمثل الانكشاف الرئيسي المقيس في الهوية: ارتباطات بأجهزة مصابة وبيانات اعتماد، وإدراج بيانات اعتماد للبيع. وكان النشاط الأبرز موجة ادعاءات DDoS في مارس لم تؤكد أي جهة رسمية انقطاعًا ناتجًا عنها. ووثّق باحثون محاولات تجسس على الحكومة والطاقة، ووجد Citizen Lab أجهزة لدى Al Jazeera استُهدفت ببرنامج تجسس وأُصيبت به. تصرّف بهذا الترتيب: تحقّق من كل تنبيه بإدراج بيانات اعتماد؛ ثم عزّز التعامل مع البريد والمرفقات؛ ثم اتفق مسبقًا على بيانات DDoS وأدوار الإبلاغ.

يجمع هذا التقرير بين ثلاثة من مصادر بيانات Brandefense الخاصة وتقارير عامة متحقق منها. فقد وفّر **Brandefense Blackhole** عدد 55,241 منشورًا مصنّفًا على أنه يخص قطر، إضافة إلى منشورات أخرى تذكر قطر أو مؤسسات قطرية، ليبلغ المجموع 74,809 منشورًا متمايزًا. كما وفّر سجلات الأجهزة المصابة وبيانات الاعتماد لـ 250 مؤسسة مختارة، وبيانات بطاقات ظهرت بنص واضح في المنشورات. ووفّر **Ransompedia** إدراجات مواقع التسريب لدى مجموعات الفدية الخاصة بقطر وأربع دول خليجية للمقارنة. واحتُسبت تصنيفات الانكشاف في **Atlas** للمؤسسات الـ 250، عبر نطاق رئيسي واحد لكل مؤسسة؛ ولم تُؤكَّد بشكل مستقل ملكية 68 من هذه النطاقات. هذه مجموعات منفصلة ولا تُجمع معًا أبدًا.

1. **انكشاف الهوية هو الخطر المقيس الأوسع انتشارًا.** لدى 182 من المؤسسات الـ 250 أجهزة مصابة مرتبطة بنطاقاتها (115,683 جهازًا في المجموع)، ولدى 213 منها سجلات تاريخية لبيانات الاعتماد (420,122 سجلًا). تشمل هذه الأعداد جميع السجلات المحفوظة في 21 نوفمبر 2026 أيًا كان تاريخ التقاطها: فهي تراكمية، وليست خاصة بعام 2026 وحده. وقد تتعلق بموظفين أو طلاب أو مرضى أو عملاء. هذه أعداد ارتباطات: أما معرفة ما إذا كان أي تسجيل دخول أو جلسة لا يزال صالحًا للاستخدام، ولمن يعود، فتتطلب التحقق. [S3][S1]

2. **بيانات الاعتماد المدرجة للبيع هي أول إشارة ينبغي فرزها.** تبلغ درجة Atlas الرئيسية للمؤسسات الـ 250 46 من 100؛ وتعني القيمة الأعلى رصد عدد أكبر من إشارات الانكشاف، ولا تعني القيمة المنخفضة أن الضوابط قوية. وكان لدى 73 من 250 مؤسسة بيانات اعتماد مرتبطة بنطاقها مدرجة للبيع وقت فحصنا، في أسواق بيانات الاعتماد التي ترصدها Brandefense. وكان لدى جميع البنوك التسعة المُصدِرة للبطاقات في قائمتنا إدراج من هذا النوع. يُنبّه الإدراج المدافع إلى البحث عن حساب نشط؛ لكنه لا يحدد عدد الحسابات ولا أصحابها. [S4]

3. **أعقبت التصعيدَ الإقليمي موجةٌ من ادعاءات هجمات DDoS من الهاكتفيست؛ ولم يُؤكَّد أي انقطاع.** بين 28 فبراير و 25 مارس ادّعت أربع مجموعات تنفيذ هجمات DDoS على بوابات حكومية ووزارات وبوابة فوترة ودفع لخدمة عامة وجهة تنظيمية مالية وموقع في قطاع الطاقة. لم نجد أي بيان من جهة رسمية قطرية أو من مؤسسة مسماة يؤكد حدوث انقطاع. وقد قاست NETSCOUT عدد 31,836 هجوم DDoS على قطر في الفترة يناير–يونيو، وصنّفت معظم الأهداف على أنها مشغلو اتصالات سلكية؛ ولا تُظهر بياناتها ما إذا كانت المواقع التي سمّتها المجموعات قد أُصيبت. [S2][S29][S32]

4. **وُثّقت محاولات تجسس، وتأكّدت إصابة أجهزة لدى جهة بث ببرنامج تجسس.** أفادت Check Point بأن Camaro Dragon المرتبطة بالصين حاولت نشر PlugX ضد أهداف قطرية خلال يوم واحد من التصعيد، مستخدمة طُعومًا تتعلق بأخبار التصعيد. وقيّمت حملة ثانية، بثقة منخفضة، على أنها متوافقة مع الصين؛ وذكر ملخصها الأسبوعي أن الحملات استهدفت جهات حكومية وأخرى مرتبطة بالطاقة. ولم تظهر أي منهما في بيانات مواقع التسريب والمنتديات التي بحثنا فيها. وبشكل منفصل، أفاد Citizen Lab في أكتوبر 2026 بأن 45 جهازًا على الأقل لدى Al Jazeera استُهدفت ببرنامج التجسس Candiru في 2024 و2025، وبأن أجهزة منها أُصيبت به (7.2§). [S26][S27][S47][S48]

5. **سمّت ادعاءات البيانات جهات في الطاقة والمصارف والأمن والتعليم؛ ولم يُؤكَّد أي منها.** ادّعى ناشران استهداف الشركة ذاتها في قطاع الطاقة في فبراير ومارس (الحالة A). وعرض بائعون بيانات موظفين لجهة أمنية حكومية (الحالة B) وسجلات عملاء نُسبت إلى بنك كبير (الحالة C). ويحتفظ Ransompedia بتسعة إدراجات لعام 2026 تخص قطر، تسمّي ثماني مؤسسات، معظمها مقاولون وشركات استشارية وموردو بنية تحتية. [S1][S6]

أربعة قرارات للقادة

1. **تعامل مع إدراجات بيانات الاعتماد الحالية كمحفّز لحادث، لا كإحصاء.** وجّه كل إدراج حالي في السوق مرتبط بنطاقاتك إلى فريق إدارة الهوية، وسجّل قرارًا بشأنه خلال 5 أيام عمل. صعّد الأمر إلى الاستجابة للحوادث عند وجود دليل على مواد مصادقة مسروقة قابلة للاستخدام، أو إساءة استخدام جلسات، أو وصول غير مصرّح به، سواء كانت المصادقة متعددة العوامل (MFA) مفعّلة أم لا. سجّل حالة MFA بوصفها عاملًا واحدًا في التحقيق. وللتصرف بناءً على ذلك، رتّب رصد إدراجات بيانات الاعتماد والأجهزة المصابة الخاصة بنطاقاتك منذ اليوم 1، عبر فريق داخلي أو مزود خدمة (12.1§).
2. **أغلق مسار المرفقات الذي استخدمه التجسس.** بُنيت حملات 2026 حول ملفات أرشيف وملفات اختصار يتعيّن على المستخدم فتحها، ثم برامج مشروعة تحمّل مكتبات خبيثة. احظر مرفقات الأرشيف والاختصارات الواردة من الخارج، وأطلق تنبيهًا عندما تحمّل ملفات تنفيذية موقّعة مكتبات DLL من مجلدات المستخدمين (7.2§).

3. **استعد لادعاءات الهاكتفيست التي تسبق الحقائق.** اتفق مسبقًا على من يؤكد حالة الخدمة علنًا خلال موجة DDoS، ورتّب مسبقًا التخفيف لدى مزود الخدمة في المنبع (upstream) للبوابات الموجهة إلى المواطنين وصفحات الدفع. ففي مارس، تداولت الادعاءات لأسابيع من دون أي بيان رسمي بشأن الانقطاعات.

4. **سمِّ شخصًا واحدًا لكل مهلة إبلاغ.** تحدد إرشادات الخصوصية 72 ساعة للاختراق الجسيم للبيانات الشخصية. ويضع المعيار الوطني وأطر المخاطر لعام 2026 أيضًا واجبات إبلاغ لم نتمكن من تأكيد مهلها؛ اطلب توضيحًا مكتوبًا من الوكالة. سمِّ المسؤول عن الإبلاغ ونائبه الآن (§10.3).

العام بالأرقام

9

إدراجات فدية مقبولة في Ransompedia تخص قطر بتاريخ 1 يناير–20 نوفمبر 2026، تسمّي 8 مؤسسات (24 على الإطلاق)

ما ليس هو
ليس عددًا للاختراقات المؤكدة؛ فالحالات غير المدرجة وغير المنشورة غير مرئية

55,241

منشورات Blackhole المصنّفة على أنها تخص قطر، 1 يناير–20 نوفمبر 2026

ما ليس هو
ليس عددًا للهجمات؛ إذ يقع 78% منها في أكتوبر ومعظمها منشورات تجنيد آلية باللغة التركية

7,867–8,175

المنشورات المصنّفة المتبقية بعد استبعاد الرسائل المزعجة والمنشورات الآلية

ما ليس هو
ليست حوادث فريدة؛ فكثير منها قوائم متعددة الدول أو يخص دولًا أخرى، لذا يُعد النطاق حدًا أعلى

31,836

هجمات DDoS على قطر قاستها NETSCOUT، يناير–يونيو 2026

ما ليس هو
ليست هجمات هاكتفيست تحديدًا؛ وصُنّفت معظم أهدافها على أنها مشغلو اتصالات

250

مؤسسة عامة وخاصة رائدة جرى تقييمها بتصنيفات Atlas، بنطاق رئيسي واحد لكل منها (68 منها مرتبطة مبدئيًا)

ما ليس هو
ليست عينة عشوائية؛ وليست تقديرًا لمعدل الانتشار الوطني

115,683

جهازًا مصابًا مرتبطًا بنطاقات هذه المؤسسات الـ 250 (4,191 منها مصنّفة كأجهزة موظفين)؛ تراكمية، وتشمل جميع السجلات المحفوظة في 21 نوفمبر 2026

ما ليس هو
ليست خاصة بعام 2026 وحده، ولا تمثل أشخاصًا فريدين، ولا إصابات حالية متحققًا منها؛ ولم تُزل منها التكرارات بين المؤسسات

420,122

سجلًا تاريخيًا لبيانات الاعتماد للنطاقات ذاتها (قواعد بيانات الاختراقات، وسجلات برامج سرقة المعلومات، وقوائم الدمج (combolist))؛ تراكمية، بصرف النظر عن تاريخ الالتقاط

ما ليس هو

ليست خاصة بعام 2026 وحده؛ ولا تمثل حسابات فريدة أو كلمات مرور نشطة

73 من 250

مؤسسة لديها بيانات اعتماد مدرجة للبيع وقت الفحص

ما ليس هو

ليس عددًا للحسابات أو للاختراقات المؤكدة

110

بطاقات دفع متمايزة مرتبطة بقطر شوهدت بنص واضح في منشورات الويب المظلم التي جُمعت (85 منسوبة إلى بنك قطري مسمّى، و 25 موسومة بأنها قطرية فقط)

ما ليس هو

ليس رقمًا لخسائر الاحتيال؛ ونطاقه ضيق (8.2§)

50%

من المؤسسات الـ 250 تطبّق DMARC (124)

ما ليس هو

ليس مقياسًا لنجاح التصيد أو لأمن التسليم

خريطة التقرير

اثنا عشر فصلاً، وخمسة مسارات للقراء. ابدأ بالصف الذي يطابق دورك؛ يفتتح كل فصل بالسؤال الذي يجيب عنه، وتُختتم الفصول 2-12 بثلاث خلاصات.

مجلس الإدارة والتنفيذيون

ماذا حدث، وما مدى تعرضنا، وما الذي ينبغي أن نقرره؟

انتقل إلى 1 3 12

مسؤول أمن المعلومات وقادة الأمن

أي حالات التعرض تخصنا، وأي الجهات الفاعلة مهمة، وأي الضوابط تأتي أولاً؟

انتقل إلى 3 6 7 9 10 12

مركز العمليات الأمنية واستخبارات التهديدات

ماذا نشرت الجهات الفاعلة، وكيف ترتبط ببعضها، وأي التقنيات استخدمها التجسس؟

انتقل إلى 4 6 7 8 12

الملحقان A-B

مكافحة الاحتيال وحماية العملاء

كيف يُتاجر بالهويات والحسابات والبطاقات القطرية، وأين تراها البنوك؟

انتقل إلى 4 5 8 9

الاتصال والشؤون القانونية

كيف نتحدث عن الادعاءات غير المتحقق منها، وأي مهل الإبلاغ تنطبق؟

انتقل إلى 6 10 12

01 **الملخص التنفيذي**
ماذا حدث في 2026 وما الذي ينبغي أن يقرره القادة أولاً

02 **السياق**
أي خصائص قطر تشكّل التهديدات

03 **التعرض الوطني**
ما مدى انكشاف 250 مؤسسة رائدة وفق تصنيفات Atlas

04 **الويب المظلم**
ماذا ينشر المجرمون عن قطر بعد إزالة الرسائل المزعجة

05 **القطاعات**
أي القطاعات تُسمّى وما الاستجابة التي يحتاجها كل منها

06 **نشاط القرصنة (الهاكتفيزم)**
ما الذي ادُّعي، وما الذي قيس، وكيف نستعد

07 **الجهات الفاعلة في التهديد**
من هي الجهات الفاعلة، وكيف ترتبط، وماذا تقول التقارير

08 **اقتصاد الاحتيال**
كيف تتحول الهويات والحسابات إلى أموال

09 **القطاع المصرفي**
أين يقع التعرض المرئي للبنوك

10 **التنظيم**
أي مهل الإبلاغ تنطبق وما الذي ينبغي فعله الآن

11 **التوقعات**
ما الذي يجب التخطيط له وما الذي قد يغيّر الخطة

12 **خطة العمل**
من يفعل ماذا خلال 90 يوماً

الفصل 2

السياق الرقمي والاستراتيجي لقطر

يجيب هذا الفصل عن

ما السمات القطرية التي تشكّل التهديدات السيبرانية الواردة في هذا التقرير، ولماذا بدا عام 2026 مختلفًا عن الأعوام السابقة؟

98.1%

نسبة انتشار الإنترنت في أكتوبر 2026، مع 4.71 مليون اتصال خلوي

في هذا الفصل

2.1 متصلة وتعتمد على الهاتف المحمول أولًا

2.2 الطاقة والطيران والمال تجتذب التجسس

2.3 نموذج خدمات رقمي ومركزي

2.4 تصعيد مارس 2026 وموجة الهاكتفيست

2.5 سلطة سيبرانية وطنية بأطر جديدة في 2026

باختصار

أربع سمات تشكّل صورة التهديدات في قطر. فالاتصال شبه شامل؛ والدور العالمي في الطاقة والطيران يجتذب التجسس؛ والخدمات رقمية ومركزية إلى حد كبير؛ وفي 2026 جلب تصعيد عسكري إقليمي موجة من ادعاءات الهاكتفيست. وتحتاج كل سمة إلى ضابط مختلف. عيّنوا مسؤولين عن رصد الهوية، وضوابط المرفقات، والتخفيف في المنبع، والتواصل بشأن حالة الخدمات.

2.1 متصلة وتعتمد على الهاتف المحمول أولًا

بلغ عدد سكان قطر نحو 3.19 مليون نسمة وعدد مستخدمي الإنترنت 3.13 مليون في أكتوبر 2026، أي بنسبة انتشار 98.1%. وكان لديها 4.71 مليون اتصال خلوي (148% من السكان) و 3.29 مليون هوية مستخدم على وسائل التواصل الاجتماعي [S9]. وفي أغسطس أعلنت هيئة تنظيم الاتصالات حصول قطر على درجة 98.4 من 100 في مؤشر ITU ICT Development Index 2026، لتحتل المرتبة السادسة بين 159 اقتصادًا. وبلغت التغطية السكانية 99% لشبكات 5G و 100% للألياف الضوئية [S10].

يهمّ هذا المستوى من الاتصال المدافعين من ناحيتين. فيمكن الوصول إلى كل مقيم وزائر تقريبًا عبر طُعوم الرسائل النصية والمراسلة والبريد الإلكتروني. كما أن عدد الأجهزة التي يمكن أن تصيبها البرمجيات الخبيثة لسرقة المعلومات كبير نسبةً إلى عدد السكان، ولهذا يهيمن انكشاف الهوية على الفصل 3.

2.2 الطاقة والطيران والمال تجتذب التجسس

كانت قطر ثاني أكبر مصدّر للغاز الطبيعي المسال (LNG) في 2024، بما يقارب 20% من صادرات الغاز الطبيعي المسال العالمية، وفقًا لإدارة معلومات الطاقة الأمريكية [S11]. وتعامل مطار حمد الدولي مع 54.3 مليون مسافر في 2025 [S12]. وتخدم البنوك وشركات التأمين ومركز قطر للمال سوقًا إقليمية.

تحتفظ المؤسسات في هذه القطاعات بمعلومات تُقدّرها جهات التجسس: العقود والتسعير والشركاء والسفر. ويتوافق نشاط التجسس الموثق لعام 2026 في مصادرنا مع هذا النمط. فقد وصفت Check Point حملتين ضد أهداف قطرية في أوائل مارس، وذكر ملخصها الأسبوعي أن الحملات استهدفت جهات حكومية وأخرى مرتبطة بالطاقة (الفصل 7) [S26][S27]. وفي أكتوبر 2026 أفاد Citizen Lab بأن 45 جهازًا على الأقل لدى Al Jazeera استُهدفت ببرنامج التجسس Candiru في 2024 و2025، وبأن أجهزة منها أُصيبت به [S47][S48].

2.3 نموذج خدمات رقمي ومركزي

تمرّ الخدمات الحكومية والمدفوعات والهوية عبر عدد صغير من المنصات الوطنية. ويشغّل مصرف قطر المركزي نظام الدفع الفوري Fawran، الذي أُطلق في 2024، وبوابة التجارة الإلكترونية QPAY [S13]. ويشغّل مزودان عالميان للحوسبة السحابية مناطق في الدوحة [S42]، وأصدر QCB لائحة للحوسبة السحابية للجهات التي يرخّصها (الفصل 10) [S23].

المنصات المركزية فعّالة، لكنها تركّز القيمة أيضًا. ويقلّدها المحتالون لأن السكان يثقون بها. وفي 2026 حذّرت كل من وزارة الداخلية والهيئة العامة للضرائب والوكالة الوطنية للأمن السيبراني الجمهور من رسائل تنتحل صفة جهات حكومية (الفصل 8) [S35][S36][S45].

2.4 تصعيد مارس 2026 وموجة الهاكتفيست

ابتداءً من 28 فبراير 2026، أعقب تصعيدًا عسكريًا في المنطقة، وفق تقارير مزودي الخدمات الأمنية، تصاعدٌ في ادعاءات هجمات DDoS من الهاكتفيست في أنحاء الخليج [S29][S30]. ووضعت Intel 471 قطر ضمن المواقع العشرة الأكثر استهدافًا بالادعاءات في الأسبوع الأول [S30]. وسجّلت NETSCOUT عدد 31,836 هجوم DDoS على قطر في الفترة يناير–يونيو 2026 [S32]، وأفادت StormWall بأن هجمات DDoS على قطر ارتفعت بنسبة 75% على أساس سنوي في الربع الأول [S31].

نصف التصعيد هنا فقط كسياق للبيانات الأمنية. ولا يتخذ هذا التقرير أي موقف من النزاع، ولا من أي حكومة معنية، ولا من العلاقات الخارجية لقطر. وتُعرض ادعاءات الهاكتفيست بوصفها ادعاءاتهم (الفصل 6).

2.5 سلطة سيبرانية وطنية بأطر جديدة في 2026

تضع الوكالة الوطنية للأمن السيبراني (NCSA)، التي أُنشئت في 2021، الاستراتيجية والمعايير الوطنية، وتعمل جهةً تنظيمية لخصوصية البيانات الشخصية [S14][S21]. وفي أكتوبر 2026 أطلقت أطرًا وطنية ومؤسسية لإدارة المخاطر [S18]. ونشرة التنبيهات العامة لديها

نشطة: فقد أحصينا أكثر من 160 تنبيهًا أمنيًا على موقعها بين يناير و 20 نوفمبر 2026، يذكر 65 منها استغلالًا نشطًا أو ثغرة يوم الصفر (zero-day) [S43]. ويعرض الفصل 10 ما تغيّر بالنسبة إلى المؤسسات.

الخلاصات الرئيسية

01

الاتصال شبه الشامل يجعل سرقة الهوية وانتحال الصفة المسار الإجرامي الافتراضي.

02

الطاقة والطيران والحكومة تجتذب تجسسًا لا يظهر في الأسواق الإجرامية.

03

جلب تصعيد مارس موجة من ادعاءات الهاكتفيست؛ تعامل معها كإشارة للتخطيط، لا كخط اتجاه.

الفصل 3

الانكشاف الوطني: 250 مؤسسة رائدة

يجيب هذا الفصل عن

ما مدى انكشاف المؤسسات العامة والخاصة الرائدة الـ 250 في البلاد عند قياسها بتصنيفات Brandefense Atlas، وما الإشارة التي ينبغي فرزها أولًا؟

73 of 250

مؤسسة كان لديها بيانات اعتماد مدرجة للبيع يوم الفحص

في هذا الفصل

3.1 بطاقة المجموعة المدروسة
3.2 درجة Atlas الرئيسية والإدراجات حسب القطاع
3.3 الأجهزة وبيانات الاعتماد
3.4 الإدراجات الحالية لبيانات الاعتماد: الإشارة الأولى للفرز
3.5 النطاقات المشابهة والمستندات المكشوفة والإشارات
3.6 نظافة البريد الإلكتروني والويب

باختصار

قيّمنا 250 مؤسسة قطرية رائدة، بنطاق رئيسي واحد لكل منها، باستخدام تصنيفات الانكشاف في Brandefense Atlas؛ ولم تُؤكَّد ملكية 68 من هذه النطاقات بشكل مستقل. لدى سبع من كل عشر منها أجهزة مصابة مرتبطة بنطاقاتها، ولدى أكثر من ثماني من كل عشر سجلات تاريخية لبيانات الاعتماد، وكان لدى ما يقارب ثلاثًا من كل عشر بيانات اعتماد مدرجة للبيع عند فحصنا. ونظافة البريد الإلكتروني والويب متفاوتة: نصفها يطبّق DMARC، ولم نرصد سجلات تفويض DNSSEC إلا لـ 6 من 250 نطاقًا. ابدأ بفرز الإدراجات الحالية، ثم أجهزة الموظفين.

3.1 بطاقة المجموعة المدروسة

البند	التعريف
المجموعة	250 مؤسسة: 52 جهة حكومية، و 30 في المصارف والمال، و 29 مجموعة تجزئة وشركات قابضة، و 24 في الإعلام والرياضة والثقافة، و 23 في التعليم والبحث، و 19 في الطاقة والمرافق، و 18 في التصنيع والصناعة، و 14 في النقل والخدمات اللوجستية، و 12 في الضيافة والسياحة، و 11 في الرعاية الصحية، و 9 في التأمين، و 9 في الاتصالات. منها 128 مملوكة للدولة، و 117 خاصة، و 5 أجنبية أو مشتركة

البند	التعريف
الاختيار	هادف: جهات الدولة والبوابات الوطنية، والبنوك المرخّصة والبنية التحتية للسوق، والمؤسسات المملوكة للدولة، والشركات المدرجة ورواد السوق. اختيرت لحجمها أو دورها النظامي، ولم تُرتّب حسب الإيرادات؛ ولم يُستخدم أي تصنيف قطري منشور لأكبر 250 مؤسسة
الوحدة	نطاق رئيسي واحد لكل مؤسسة. جميع النطاقات الـ 250 تُحلّ في DNS (21 نوفمبر 2026). وفي 182 نطاقًا أمكن فحص صفحتها الرئيسية، تطابقت الصفحة مع المؤسسة. أما ارتباط النطاقات الـ 68 الأخرى بمؤسساتها فمبدئي: لم تُؤكَّد ملكيتها بشكل مستقل، وتُنسب نتائجها بهذا التحفظ
القياسات	الأجهزة المصابة وأجهزة الموظفين، وسجلات قواعد بيانات الاختراقات وسجلات برامج سرقة المعلومات وقوائم الدمج (combolist)، والإشارات في دردشات ومنتديات الويب المظلم، والنطاقات المشابهة، والمستندات المكشوفة، والإدراجات الحالية في أسواق بيانات الاعتماد، باستخدام البيانات ذاتها التي يستخدمها Atlas؛ إضافة إلى فحوص عامة لـ DNS وTLS وترويسات HTTP
التاريخ	قُرئت أعداد الأجهزة وبيانات الاعتماد والإدراجات في 21 نوفمبر 2026؛ وهي جميع السجلات المحفوظة في ذلك التاريخ، بصرف النظر عن تاريخ الالتقاط (تراكمية، وليست خاصة بعام 2026 وحده). وتغطي أعداد الإشارات الفترة 19 نوفمبر 2025–18 نوفمبر 2026؛ وتغطي أعداد النطاقات المشابهة الفترة 19 أكتوبر–18 نوفمبر 2026
لم تُزل التكرارات	لا بين المصادر، ولا بين المؤسسات، ولا بين الأشخاص. فقد يظهر شخص واحد في عدة مصادر؛ وقد يحتوي جهاز واحد على بيانات دخول لعدة مؤسسات
ليست تمثيلية	تصف النتائج هذه القائمة. وهي ليست معدلات انتشار وطنية

3.2 درجة Atlas الرئيسية والإدراجات حسب القطاع

يقيّم Atlas كل مؤسسة من 0 (لم يُرصد أي خطر) إلى 100 استنادًا إلى عدة إشارات. ومنها الأجهزة المصابة، وأجهزة الموظفين، وسجلات اختراقات الأطراف الثالثة، والإشارات في الدردشات المظلمة، والإشارات في الويب المظلم، والنطاقات المشابهة، والمستندات المكشوفة، وبيع البيانات.

كيف تُقرأ تصنيفات Atlas.

المصطلح	المعنى
الدرجة الرئيسية	درجة Atlas الملخّصة على مستوى الدولة (جميع المؤسسات الـ 250)؛ وهي ليست متوسطًا
إدراج حالي	بيانات اعتماد مرتبطة بالنطاق معروضة للبيع وقت الفحص

بيانات الاعتماد والأجهزة المصابة شائعة في معظم القطاعات

حصة المؤسسات في كل قطاع التي تظهر لديها الإشارة. تظهر الإدراجات الحالية لبيانات الاعتماد باللون المرجاني.

	المستندات المكشوفة	النطاقات الشبيهة (30 يوماً)	سجل الإدراجات	الإدراج الحالي	سجلات بيانات الاعتماد	أجهزة الموظفين	الأجهزة المصابة
الإعلام والرياضة والثقافة (24)	46%	75%	46%	50%	92%	71%	88%
الرعاية الصحية (11)	45%	27%	9%	45%	82%	64%	73%
الاتصالات (9)	56%	67%	22%	44%	89%	89%	89%
النقل والخدمات اللوجستية (14)	50%	57%	36%	43%	86%	64%	86%
المصارف والمال (30)	40%	60%	23%	40%	70%	30%	60%
الطاقة والمرافق (19)	37%	53%	16%	32%	84%	58%	58%
التعليم والبحث (23)	39%	65%	13%	26%	100%	87%	91%
الحكومة (52)	42%	83%	19%	25%	94%	73%	92%
التجزئة والشركات القابضة (29)	48%	48%	3%	24%	90%	66%	69%
التأمين (9)	22%	56%	11%	11%	67%	33%	44%
التصنيع والصناعة (18)	33%	39%	6%	6%	67%	33%	39%
الضيافة والسياحة (12)	25%	17%	0%	0%	75%	8%	33%

المصدر: ارتباطات Brandefense Blackhole وتصنيفات Atlas لـ 250 مؤسسة، قُرئت في 21 نوفمبر 2026 [S3][S4]. السجلات تراكمية، وليست خاصة بعام 2026 وحده.

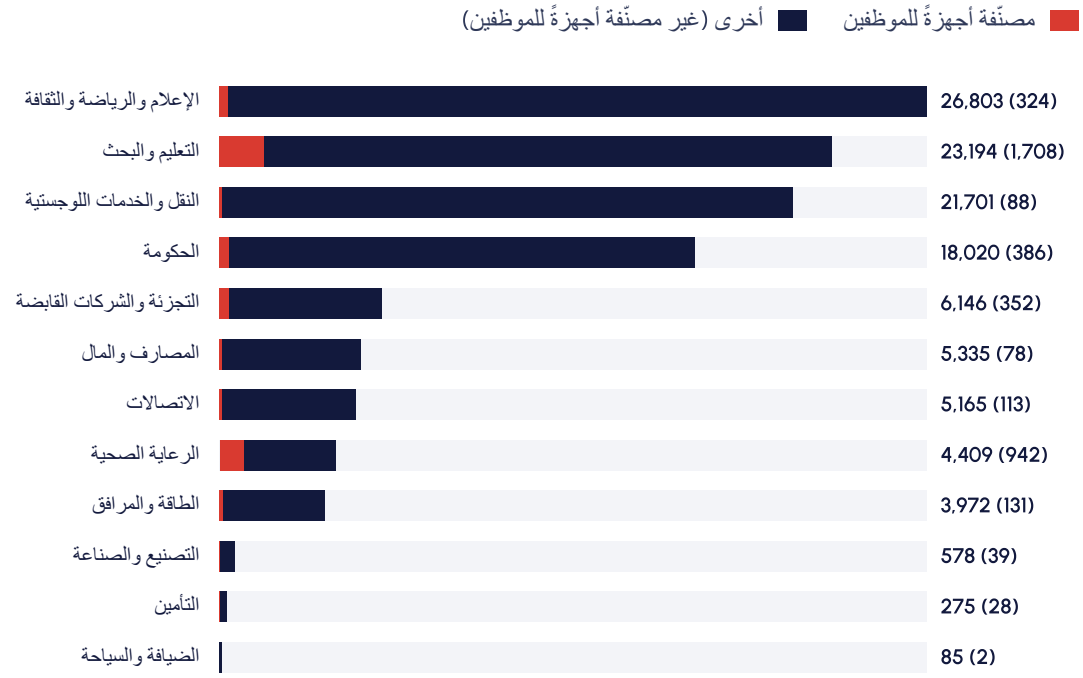
القطاع	المؤسسات	مؤسسات لديها إدراج حالي لبيانات اعتماد
الحكومة	52	13
المصارف والمال	30	12
التجزئة والشركات القابضة	29	7
الإعلام والرياضة والثقافة	24	12
التعليم والبحث	23	6
الطاقة والمرافق	19	6
التصنيع والصناعة	18	1
النقل والخدمات اللوجستية	14	6

القطاع	المؤسسات	مؤسسات لديها إدراج حالي لبيانات اعتماد
الضيافة والسياحة	12	0
الرعاية الصحية	11	5
التأمين	9	1
الاتصالات	9	4
جميع المؤسسات الـ 250	**250**	**73**

قراءة الجدول. تصف الأعداد هذه القائمة، لا كل قطاع على المستوى الوطني. وتبلغ درجة Atlas الرئيسية الوطنية لجميع المؤسسات الـ 250 46 من 100. وتعني الدرجة الأعلى رصد عدد أكبر من إشارات الانكشاف؛ أما الدرجة المنخفضة فتعني رصد إشارات قليلة، لا أن الضوابط قوية (انظر §3.6).

3.3 الأجهزة وبيانات الاعتماد

الإعلام والتعليم والنقل تحمل أكبر عدد من ارتباطات الأجهزة المصابة؛ والتعليم والرعاية الصحية تضمّان معظم الأجهزة المصنّفة كأجهزة موظفين



المصدر: ارتباطات Brandefense Blackhole وتصنيفات Atlas لـ 250 مؤسسة، قُرئت في 21 نوفمبر 2026 [S4][S3]. السجلات تراكمية، وليست خاصة بعام 2026 وحده.

القطاع	مؤسسات لديها أجهزة مصابة	الأجهزة (الموظفين)	سجلات بيانات الاعتماد	حصة سجلات بيانات الاعتماد ل
الإعلام والرياضة والثقافة	21 من 24	26,803 (324)	36,274	72%
التعليم والبحث	21 من 23	23,194 (1,708)	192,723	75%
النقل والخدمات اللوجستية	12 من 14	21,701 (88)	22,321	77%
الحكومة	48 من 52	18,020 (386)	25,502	24%
التجزئة والشركات القابضة	20 من 29	6,146 (352)	24,271	49%
المصارف والمال	18 من 30	5,335 (78)	15,049	45%
الاتصالات	8 من 9	5,165 (113)	10,165	72%
الرعاية الصحية	8 من 11	4,409 (942)	74,475	89%
الطاقة والمرافق	11 من 19	3,972 (131)	10,002	46%
التصنيع والصناعة	7 من 18	578 (39)	7,391	66%
التأمين	4 من 9	275 (28)	1,149	77%
الضيافة والسياحة	4 من 12	85 (2)	800	85%
الكل	**182 من 250**	**115,683 (4,191)**	**420,122**	**44%**

تنقسم سجلات بيانات الاعتماد إلى 116,273 سجلًا من قواعد بيانات الاختراقات، و 118,099 سطرًا من سجلات برامج سرقة المعلومات، و 185,750 إدخالًا من قوائم الدمج (combolist). وتحتوي الأجهزة المصابة على نحو 1.98 مليون بيانات اعتماد ملتقطة في المجموع، لجميع الخدمات، لا لخدمات المؤسسة وحدها.

ماذا يعني ذلك.

- **تقع معظم ارتباطات الأجهزة خارج تصنيف الموظفين.** 111,492 من الأجهزة الـ 115,683 ليست مصنّفة كأجهزة موظفين. وتتضمن سجلات برامج سرقة المعلومات الخاصة بها تسجيل دخول إلى موقع المؤسسة، ولذلك فالأرجح أنها أجهزة كمبيوتر خاصة بالعملاء أو الزوار، وإن لم تُثبت ملكيتها. وتمثل هذه الارتباطات إشارة إلى الاحتيال والاستيلاء على الحسابات، ولا تثبت بحد ذاتها وقوع اختراق. أما الأجهزة الـ 4,191 المصنّفة كأجهزة موظفين فهي المجموعة الفرعية ذات الصلة بالاختراق؛ وكلتا المجموعتين تتطلب التحقق.
- **تتركز مشكلة أجهزة الموظفين في الجامعات والمستشفيات.** لدى قطاع التعليم 1,708 أجهزة مصنّفة كأجهزة موظفين، أي 41% من الإجمالي الوطني في قائمتنا، وأكبر عدد من بيانات الاعتماد. ولدى الرعاية الصحية 942. وفي كلا القطاعين قد يتشارك الموظفون والطلاب والمرضى النطاقات، ولذلك قد تشملهم فئة "الموظفين".
- **يتفاوت التركّز.** في الرعاية الصحية، تحتفظ مؤسستان بنسبة 89% من سجلات بيانات الاعتماد؛ وفي الحكومة تحتفظ أكبر مؤسستين بنسبة 24%. ولذلك فإن إجمالي القطاع دليل ضعيف على المؤسسة النموذجية.
- **المؤسسة الوسيطة متواضعة.** لدى المؤسسة الوسيطة 9 أجهزة مصابة و 196 سجلًا لبيانات الاعتماد. أما أثقل المؤسسات منفردةً فتحمل آلاف الأجهزة أو عشرات الآلاف من سجلات بيانات الاعتماد.

3.4 الإدراجات الحالية لبيانات الاعتماد: الإشارة الأولى للفرز

كان لدى 73 من 250 مؤسسة بيانات اعتماد واحدة على الأقل مرتبطة بنطاقها مدرجة في سوق مرصود لبيانات الاعتماد وقت الفحص. ومن بين هذه المؤسسات الـ 73، لدى 45 أيضًا سجل إدراجات سابق.

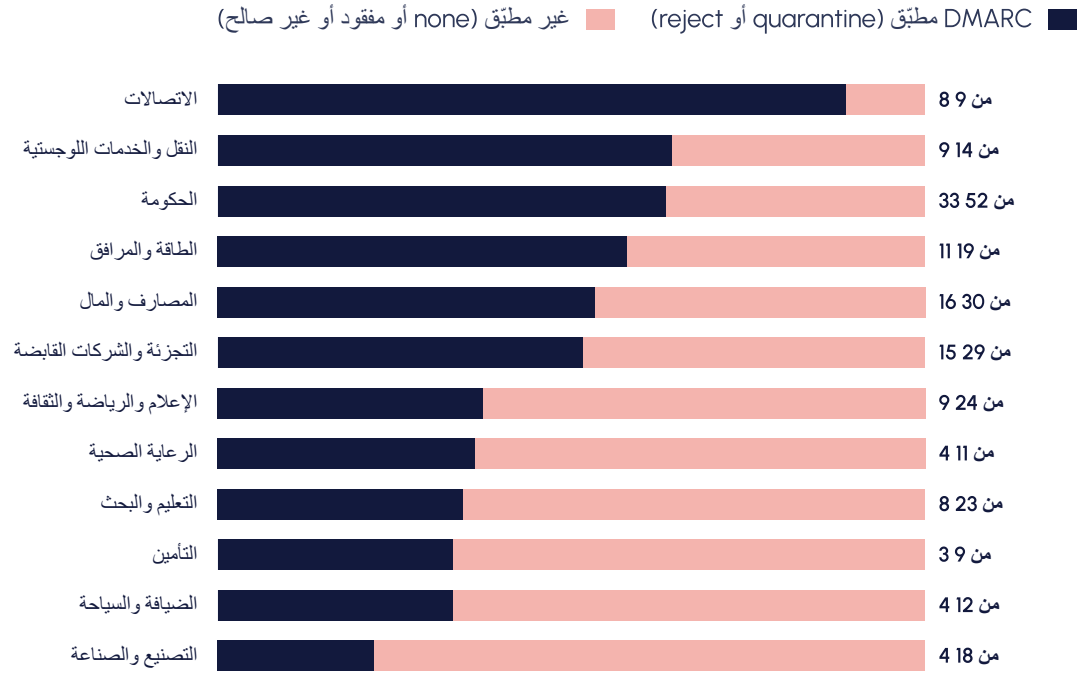
بالنسبة إلى المدافع، فإن الإدراج الحالي هو أكثر إشارات السوق مباشرةً على أن بيانات دخول مرتبطة بالنطاق معروضة. أما ما إذا كانت بيانات الدخول تلك لا تزال تعمل فهو ما يجب أن يثبته التحقق. فالإدراج لا يحدد عدد الحسابات، ولا أصحابها، ولا ما إذا كان الحساب نشطًا، أو محميًا بالمصادقة متعددة العوامل، أو أُعيد تعيينه بالفعل. والقرار الذي يدعمه هو "تحقّق من الحساب الآن"، لا "أعلن وقوع اختراق".

3.5 النطاقات المشابهة والمستندات المكشوفة والإشارات

- **النطاقات المشابهة:** عُثر على نطاقات مشابهة رُصدت حديثًا خلال الأيام الـ 30 المنتهية في 18 نوفمبر لدى 149 مؤسسة. والنطاقات المشابهة مرشّحة، وليست مواقع تصيد مؤكدة.
- **المستندات المكشوفة:** لدى 103 مؤسسات مستند مكشوف واحد على الأقل يشير إلى نطاقها (359 في المجموع).
- **الإشارات:** ذُكرت 41 مؤسسة في مصادر الدردشات المظلمة خلال الأيام الـ 365 الأخيرة، و 17 في مصادر الويب المظلم (onion). الأعداد صغيرة؛ وأعلى عدد لأي مؤسسة منفردة هو 36. وتقيس أعداد الإشارات الظهور، لا العدائية.

3.6 نظافة البريد الإلكتروني والويب

الاتصالات والنقل والحكومة تطبّق DMARC في الغالب؛ والتصنيع والتأمين والضيافة لا تطبّقه في الغالب



المصدر: فحوص Brandefense العامة لـ DNS وTLS والصفحة الرئيسية لـ 250 نطاقاً، 21 نوفمبر 2026 [S5].

نتائج فحوصنا العامة لـ DNS وTLS والصفحات الرئيسية [S5]:

الضابط	النتيجة (من 250 ما لم يُذكر خلاف ذلك)	القراءة
DMARC reject	47	يُفترض رفض البريد المنتحَل الصادر باسم النطاق
DMARC quarantine	77	يُفترض أن يذهب البريد المنتحَل إلى البريد المزعج
DMARC p=none أو مفقود	126 (57 none، و 69 مفقود)	لا تطبيق؛ وانتحال النطاق أسهل
SPF ينتهي بـ -all / ~all / ?all / غير ذلك / لا شيء	154 / 52 / 1 / 4 / 39	39 نطاقًا لا تنشر أي سياسة SPF
DKIM مرصود	147	عدم رصد DKIM ليس دليلًا على غيابه
رُصد سجل DS (تفويض DNSSEC)	6	لم يُرصد سجل DS لـ 244 نطاقًا؛ وسجل DS وحده لا يثبت وجود سلسلة ثقة صالحة

الضابط	النتيجة (من 250 ما لم يُذكر خلاف ذلك)	القراءة
شهادة TLS غير صالحة	23 من 220 نطاقًا جرى تقييمها (30 لم تُقيَّم)	عُثر على شهادات منتهية الصلاحية أو غير متطابقة أو غير موثوقة
HSTS على الصفحة الرئيسية	93 من 182 يمكن الوصول إليها	كثير من المواقع لا تفرض HTTPS على الزوار العائدين
مزود البريد	107 Microsoft 365، و 10 Google، و 37 بلا سجل MX	البقية تشغّل بريدها الخاص أو بريدًا إقليميًا

لم تكن فحوص الصفحة الرئيسية متاحة لـ 68 موقعًا، ولا فحوص TLS لـ 30 موقعًا. أما فحوص DNS فمكتملة للنطاقات الـ 250 جميعها.

الاتصالات والنقل في الصدارة؛ والتصنيع متأخر. تطبّق 8 من 9 مؤسسات اتصالات DMARC، وكذلك 9 من 14 في النقل و 33 من 52 جهة حكومية. أما التصنيع (4 من 18) والتأمين (3 من 9) والضيافة (4 من 12) فهي الأقل تطبيقًا، ويليها عن قرب التعليم (8 من 23) والرعاية الصحية (4 من 11) والإعلام (9 من 24). ويقع قطاع المصارف في الوسط بـ 16 من 30. وعلى مؤشر النظافة السلبي (الملحق A.5؛ من 0–100، والأعلى أضعف)، يسجّل التصنيع والتعليم (56 لكل منهما) أضعف قيم المؤشر القطاعية، والاتصالات (34) أقواها.

توقيع DNS شبه غائب. لا يُظهر سوى 6 من 250 نطاقًا رئيسيًا سجل تفويض DNSSEC. وهذا يترك إجابات DNS الخاصة بالبوابات الوطنية والبنوك وشركات الطاقة غير موثّقة بالنسبة إلى المحلِّلات (resolvers) التي تجري التحقق.

الخلاصات الرئيسية

01

ارتباطات الأجهزة المصابة وبيانات الاعتماد واسعة الانتشار في القائمة؛ وهي تستدعي التحقق، لا الذعر.

02

كان لدى 73 من 250 مؤسسة بيانات اعتماد مدرجة للبيع وقت الفحص؛ والإدراجات هي أول بند يجب فرزه.

03

نصف النطاقات لا تطبّق DMARC، ولا ينشر سوى 6 من 250 تفويض DNSSEC.

الفصل 4

ما نراه على الويب المظلم

يجيب هذا الفصل عن

ما الذي ينشره المجرمون فعلًا عن قطر بعد إزالة الرسائل الآلية المزعجة، وأي العروض تهم المدافعين؟

7,867-8,175

منشورًا منقّحًا تبقى من أصل 55,241 منشورًا موسومًا

في هذا الفصل

4.1 بطاقة النطاق | 4.2 المنصات واللغات والحجم | 4.3 عائلات الجريمة بعد التنقيح | 4.4 ادعاءات محددة ضد مؤسسات قطرية

4.5 دراسات حالة | 4.6 ما تضيفه المنتديات

باختصار

معظم الحركة السرية الموسومة بقطر إعلانات جماعية، وقد بلغت منشورات التجنيد الآلية الناطقة بالتركية وحدها 41,000 منشور في أكتوبر. بعد التنقيح يتبقى نحو 8,000 منشور. تظهر قطر في الغالب سوقًا واحدة بين أسواق كثيرة في قنوات بطاقات الدفع المسروقة (carding) والهويات وتداول الحسابات. وعدد قليل من المنشورات يطرح ادعاءات محددة ضد جهات قطرية في الطاقة والمصارف والأمن والتعليم والقطاع العام. يجب فرز كل ادعاء بحسب مصدره وعيّنته وعمره قبل أن يتحدث أحد عن اختراق.

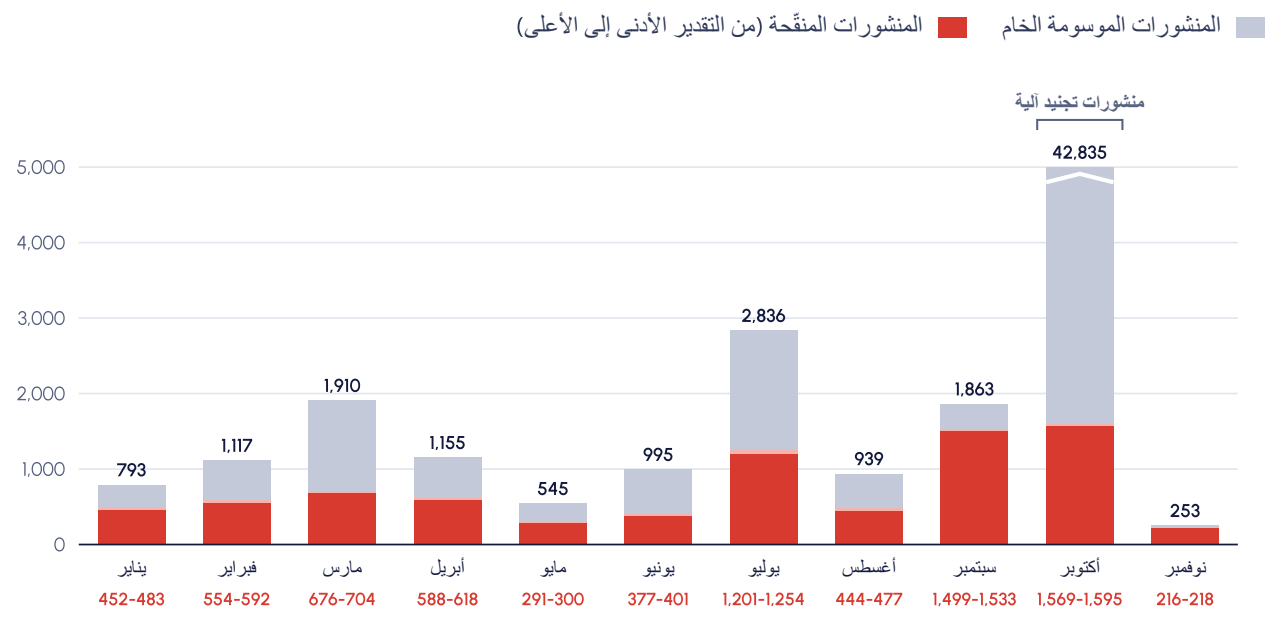
4.1 بطاقة النطاق

البند	التعريف
المصدر	Brandefense Blackhole: قنوات ومجموعات Telegram، ومجموعة من منتديات الجرائم الإلكترونية، ومواقع اللصق وDiscord، تُجمع بصورة مستمرة
تعريف الدولة	منشورات موسومة بأنها تخص قطر ("هذا المنشور يتناول قطر أو يستهدفها أو يذكرها")، إضافة إلى منشورات تذكر قطر أو مؤسسات قطرية
النافذة الزمنية	وقت النشر 1 يناير–20 نوفمبر 2026 (نوفمبر جزئي). لا يُستخدم وقت الجمع مطلقًا

البند	التعريف
المجموعة الموسومة	55,241 منشورًا
المدوّنة المجمّعة	74,809 منشورات متمايزة موسومة بقطر أو تذكرها
المنشورات المنقّاة	المنشورات المتبقية بعد استبعاد الرسائل المزعجة والمنشورات الآلية (الملحق A.2)
ما لا يثبته ذلك	أن منشورًا موسومًا يستهدف قطر، أو أن ادعاءً ما صحيح، أو أن منشورين يتعلقان بالملف نفسه

4.2 المنصات واللغات والحجم

منشورات آلية في أكتوبر تضخّم العدد الخام؛ ويبقى الحجم المنقّح بين 291 و 1,595 منشورًا في كل شهر مكتمل

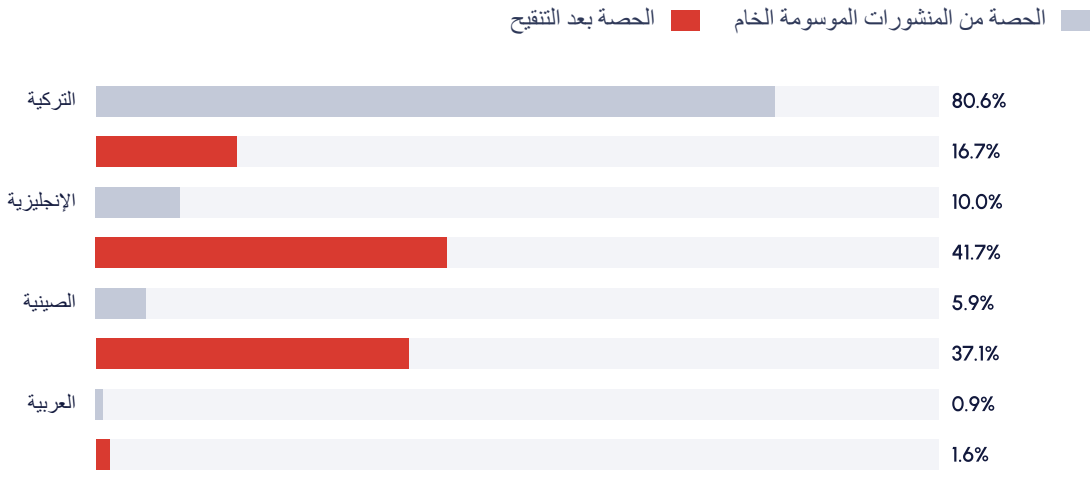


المصدر: Brandefense Blackhole، المنشورات الموسومة بأنها تتعلق بقطر، تواريخ النشر 1 يناير–20 نوفمبر 2026، ونوفمبر جزئي [S1]. أعداد المنشورات المنقّحة حدّ أعلى.

المقياس	القيمة
حصة Telegram من المنشورات الموسومة	99.7% (55,095)
منشورات المنتديات	90 (إضافة إلى 334 منشورًا آخر في المنتديات يذكر قطر)

المقياس	القيمة
مواقع اللصق وDiscord ومواقع onion	23، 33، 0
التركية / الإنجليزية / الصينية / الروسية / العربية	80.6% / 10.0% / 5.9% / 1.4% / 0.9% من المنشورات الخام
بعد التنقيح: الإنجليزية / الصينية / التركية / العربية	41.7% / 37.1% / 16.7% / 1.6%
المنشورات الخام شهريًا	42,835 في أكتوبر؛ و 253–2,836 في الأشهر الأخرى

التركية تهيمن على الوسم الخام؛ وبعد التنقيح تحمل المنشورات الإنجليزية والصينية معظم الوزن



يحمل Telegram نسبة 99.7% من المنشورات الموسومة. المصدر: Brandefense Blackhole، المنشورات الموسومة بأنها تتعلق بقطر، تواريخ النشر 1 يناير–20 نوفمبر 2026، ونوفمبر جزئي [S1]. أعداد المنشورات المنقّحة حدّ أعلى.

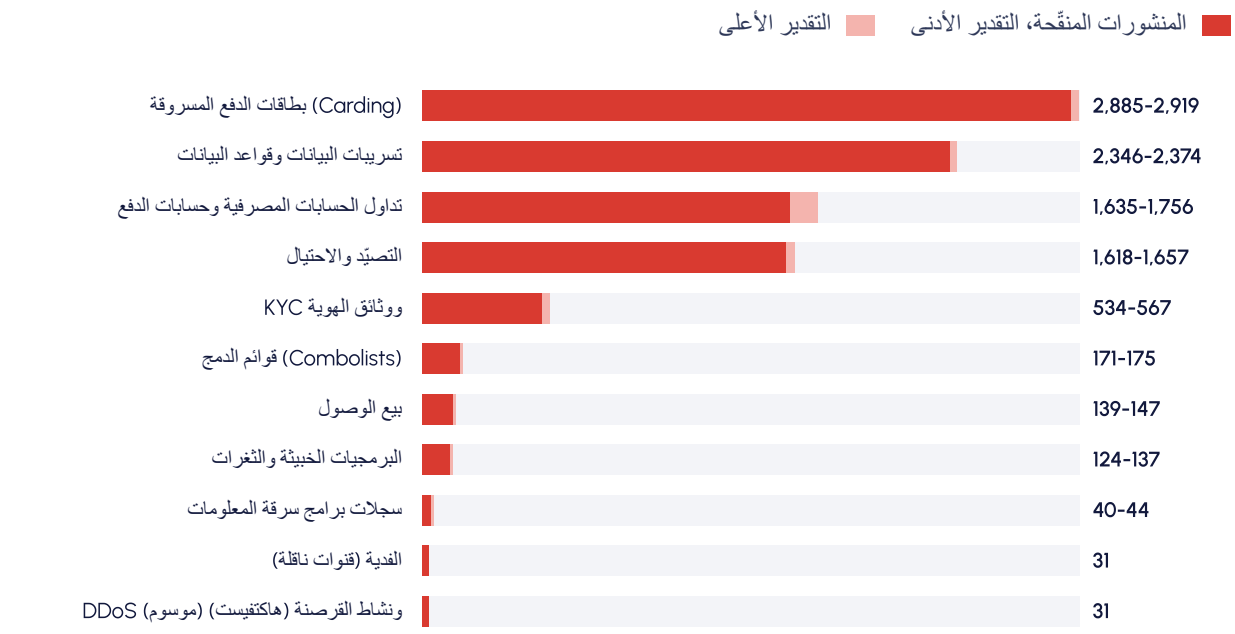
ذروة أكتوبر ليست موجة هجمات. يقع 78% من المنشورات الموسومة خلال العام في أكتوبر، و 41,438 منها بالتركية. وهي إعلانات تجنيد آلية لحسابات مصرفية تركية، نُشرت في مئات المحادثات ووُسمت بقطر. وبعد استبعاد الرسائل المزعجة والمنشورات الآلية يضم أكتوبر 1,569–1,595 منشورًا منقّحًا، وهو مستوى يتماشى مع يوليو وسبتمبر.

يبدو أن الجمع انخفض منذ منتصف العام. ينخفض الحجم الموسوم لتركيا أيضًا انخفاضًا حادًا بين مايو ويوليو. لذلك لا نقرأ التراجعات منذ منتصف العام على أنها اتجاهات في التهديد.

العربية شبه غائبة. تشكّل المنشورات العربية أقل من 2% من المدوّنة المنقّحة. تجري التجارة الإجرامية ذات الصلة بقطر في مجموعتنا في الغالب بالإنجليزية والصينية، في قنوات تخدم دولًا كثيرة. أما المجموعات المغلقة الناطقة بالعربية فهي خارج نطاق جمعنا (الملحق A.8).

4.3 عائلات الجريمة بعد التنقيح

منشورات بطاقات الدفع المسروقة وتسريبات البيانات تتصدر المدوّنة المنقّحة؛ يليها تداول الحسابات والتصيّد وخدمات الهوية



المصدر: Brandefense Blackhole، المنشورات الموسومة بأنها تتعلق بقطر، تواريخ النشر 1 يناير–20 نوفمبر 2026، ونوفمبر جزئي [S1]. أعداد المنشورات المنقّحة حدّ أعلى.

العائلة	المنشورات المنقّحة (الأدنى–الأعلى)	ما تحتويه
بطاقات الدفع المسروقة (Carding)	2,885–2,919	تحديثات متاجر البطاقات التي تدرج قطر بين عشرات الدول، ومخرجات أدوات الفحص التي تسمّي جهات إصدار قطرية، ومشترون لبطاقات "الشرق الأوسط"
تسريبات البيانات وقواعد البيانات	2,346–2,374	"قواعد" متاجر البطاقات، وقوائم عملاء محتملين خليجية، وعروض قواعد بيانات تسمّي مؤسسات قطرية
تداول الحسابات المصرفية وحسابات الدفع	1,635–1,756	تأجير الحسابات وبيعها؛ ويتعلق كثير من المنشورات بمصرف تركي، لا بمصرف قطري
التصيّد والاحتيال	1,618–1,657	صفحات احتيال، وخدمات الرسائل النصية وانتحال هوية المتصل التي تدرج قطر، ومشترون لحسابات مسجلة في قطر
KYC ووثائق الهوية	534–567	حسابات موثّقة على منصات تداول "لقطر"، وقوالب وثائق، وخدمات تحقق

العائلة	المنشورات المنقّحة (الأدنى-الأعلى)	ما تحتويه
قوائم الدمج (Combolists)	171–175	قوائم بيانات اعتماد موسومة بالدولة والنطاق، بما فيها حسابات برامج ولاء شركات طيران
بيع الوصول	139–147	وصول عن بُعد ولوحات تحكم ومشترون يطلبون وصولًا حكوميًا
البرمجيات الخبيثة والثغرات	124–137	بيع أدوات ونقاش حول الثغرات، عالمي في معظمه
سجلات برامج سرقة المعلومات	40–44	بيع سجلات تسمّي خدمات قطرية
الفدية (قنوات ناقلة)	31	روبوتات تتبّع تنقل ادعاءات مواقع التسريب (الفصل 7)
DDoS ونشاط القرصنة (هاكتفيست) (موسوم)	31	ضئيل ضمن الوسم؛ ويستند الفصل 6 إلى قنوات الجهات الفاعلة والتقارير العامة

تتداخل العائلات ولا يجوز جمعها. وكثير من المنشورات المنقّحة قوائم متعددة الدول أو يخص مصرفًا تركيًا لا قطر. تعامل مع الأعداد المنقّحة على أنها حد أعلى.

الأسعار المعلنة. في المنشورات المنقّحة، بلغ الوسيط للسعر المعلن 14 USD للبطاقة، و 15 USD لعروض البيانات والعملاء المحتملين، و 32 USD للحسابات المصرفية والمحافظ، و 50 USD لخدمات KYC والوثائق. هذه أسعار مطلوبة وليست عمليات بيع مكتملة (الفصل 8).

4.4 ادعاءات محددة ضد مؤسسات قطرية

تبرز ستة عشر عرضًا لأنها تسمّي مؤسسة قطرية أو قطاعًا قطريًا وتدّعي امتلاك وصول أو بيانات. لم يُتحقق من أي منها بشكل مستقل، ولم نحصل على أي ملف.

التاريخ	الهدف المزعوم	الادعاء	المنصة	المنشور
17 يناير	جهة في القطاع المالي	"قاعدة بيانات مالية" من 800,000 سطر بسعر 400 دولار أمريكي	قناة Telegram	لا يوجد
5 فبراير	مقاول هندسي في قطاع الطاقة	قاعدة بيانات تضم أسماء وبيانات اتصال ومستندات وجوازات سفر	قناة Telegram لمجموعة تسمي نفسها LulzSec Hackers	لا يوجد

التاريخ	الهدف المزعوم	الادعاء	المنصة	المنشور
19 فبراير	شركة في قطاع الطاقة	وصول حي إلى أنظمة السحابة والهوية؛ وسجلات للموظفين	منتدى اختراقات	B01
3 مارس	جهة في قطاع الطيران	قاعدة بيانات معروضة في قناة خاصة	نقل عبر أداة رصد تسريبات	لا يوجد
9 مارس	بيانات مدنية لقطر وأربع أسواق أخرى	560 GB من السجلات الشخصية وسجلات الشركات "الحديثة"	قناة Telegram ناطقة بالعربية	B17
10 مارس	شركة قطاع الطاقة نفسها	"تفريغ" لقاعدة بيانات يضم سجلات للموظفين؛ ويقول الناشر إنه مسح خادمًا	قناة Telegram	B02
10 مارس	جهة أمنية حكومية	بيانات أفراد عن 1,900 عضو، مقابل 10,000 USD	منتديا اختراقات؛ ونقل عبر Telegram	B03
16 مايو	تطبيق خصومات استهلاكي	نحو 300,000 سجل مستخدم من اختراق يؤرخه الناشر في 2023	منتدى؛ ونقل سابق في يناير ومارس	B18
19 مايو-22 يوليو	مستشفى خاص	نحو 12 GB يُقال إنها تضم سجلات مرضى وتأمين (مايو)، ثم نحو 31,000 ملف سيرة ذاتية لكوادر طبية (يوليو)	نقل عبر Telegram لإدراجين	B16
8 يونيو	مجموعة مدارس خاصة	أكثر من 100 GB، تشمل جوازات سفر وبطاقات هوية وبيانات موظفين؛ ويقول الناشر إنه حذف قواعد البيانات	منتدى اختراقات	B06
16 يونيو	شركة فعاليات	قاعدة بيانات مستخدمين تضم رسائل بريد إلكتروني وكلمات مرور وأرقام هواتف	منتدى	لا يوجد
25 يوليو	متسوقون عبر الإنترنت	"بيانات تسوّق قطر"، 36,000 سجل	نقل عبر أداة رصد تسريبات	لا يوجد
26 أغسطس	مصرف كبير	مجموعة بيانات يُقال إنها تمتد على 2024-2026، تشمل سجلات حكومية ودفاعية	نقل عبر Telegram لإدراج في منتدى	B05

التاريخ	الهدف المزعوم	الادعاء	المنصة	المنشور
3 سبتمبر	جهة في القطاع العام	صفوف عيّنة تتضمن رموز وصول إلى التطبيقات	منتدى	B07
10–14 نوفمبر	المصرف الكبير نفسه	عدد كبير جدًا من سجلات العملاء وسجلات للموظفين، مقابل 1,500 USD	منتديا اختراقات	B04
16 نوفمبر	نادٍ رياضي	108 ملفات تضم بطاقات هوية وجوازات سفر وعقود لاعبين وبيانات مصرفية، من اختراق يؤرخه الناشر بعام 2025	منتدى	لا يوجد

ما يعنيه ذلك للمدافعين. تتركز الادعاءات على مؤسسات تضم أعدادًا كبيرة من الموظفين أو العملاء: الطاقة والمصارف والأمن والتعليم والقطاع العام. يُظهر زوجان من الحالات تكرارًا لا تأكيدًا مستقلًا. فقد سمّى ناشران مختلفان شركة قطاع الطاقة بفارق ثلاثة أسابيع وبأرقام مختلفة. وسُمّي المصرف الكبير في أبريل وأغسطس ونوفمبر؛ ويرد موضوع أبريل في الحالة C وليس ضمن العروض الستة عشر. التكرار يرفع أولوية التحقق؛ لكنه لا يثبت وقوع اختراق.

كما أن عدة ادعاءات غير معقولة بمنطقها الخاص. يدّعي أحد البائعين امتلاك ملف عملاء كبير جدًا لكنه يسعّره بـ 1,500 USD. ويؤرخ آخر ملفه في 2023 بينما يبيعه على أنه جديد. ولا يثبت أي من هذين التفصيلين أن الادعاء ملفّق.

بطاقة الدليل B01 — 19 فبراير 2026

Unnamed poster (a public monitor names Montaro)

منتدى تسريبات · Forum · الإنجليزية

النص الأصلي

```
TARGET PROFILE Entity: [energy-sector company] [...] Status: Active Session - All Systems Accessible [...] Employee registry extracted [...] Cloud credentials discovered in connection strings [...] Global Administrator privileges obtained [...]
```

الترجمة

ملف الهدف: الجهة: [شركة في قطاع الطاقة] [...] الحالة: جلسة نشطة - جميع الأنظمة متاحة [...] استُخرج سجل الموظفين [...] اكتُشفت بيانات اعتماد سحابية في سلاسل الاتصال [...] تم الحصول على صلاحيات المسؤول العام (Global Administrator) [...]

ما يمكن إثباته	الادعاء وجدوله الزمني المزعوم وأنواع الأنظمة التي يذكرها (السحابة، دليل الهويات، أمن المباني)؛ ونقل جهة رصد عامة لادعاء مشابه قبل يوم واحد.
ما لم يثبت	أي وصول أو سرقة بيانات؛ أو ما إذا كان الناشر هو الشخصية التي تسميها جهة الرصد.

بطاقة الدليل B02 — 10 مارس 2026

ELIPHAS SYNDICATE

Telegram · قناة Telegram · الإنجليزية

النص الأصلي

```
WE JUST PULLED A MASSIVE RELIABLE DUMP FROM [energy-sector company] [...] WE WIPED THE WHOLE SERVER CLEAN AFTER EXFILTRATION [...] INCLUDING [...] FULL EMPLOYEE RECORDS [...] WE DONT CARE ABOUT THE POLITICS WE CARE ABOUT THE PAYOUT
```

الترجمة

سحبنا للتو تفريغًا ضخمًا وموثوقًا من [شركة في قطاع الطاقة] [...] مسحنا الخادم بالكامل بعد الاستخراج [...] بما في ذلك [...] سجلات كاملة للموظفين [...] لا تهمنا السياسة، يهمنا المال

ما يمكن إثباته	الادعاء وأنواع السجلات المزعومة، والدافع المالي الذي أعلنه الناشر.
ما لم يثبت	أي مسح أو استخراج للبيانات، أو صلة بناشر فبراير.

بطاقة الدليل B03 — 10 مارس 2026

TheAshborn منتدى تسريبات · Forum · الإنجليزية

النص الأصلي

```
We had Access to [government security body] [...] We Sell 1900X personnel data (Dumped data) 2 Screenshots as proof: [link removed] Data includes: {Full Name Email Business Fixed Number Home Fixed Number Mobile Number Fax Number Job Title Department Company Nationality} Price : 10,000$
```

الترجمة

كان لدينا وصول إلى [جهة أمنية حكومية] [...] نبيع بيانات 1900X من الموظفين (بيانات مفرّغة) 2 لقطة شاشة كدليل: [تمت إزالة الرابط] تشمل البيانات: {الاسم الكامل، البريد الإلكتروني، رقم العمل الثابت، رقم المنزل الثابت، رقم الجوال، رقم الفاكس، المسمى الوظيفي، القسم، الشركة، الجنسية} السعر: 10,000$

ما يمكن إثباته — العرض والحقول المزعومة والسعر ونسختان على المنتدى في اليوم نفسه.

ما لم يثبت — مصدر البيانات أو عمرها، أو أي عملية بيع.

بطاقة الدليل B17 — 9 مارس 2026

Data seller قناة Telegram · Telegram

العربية، مع نص روسي وإنجليزي من البائع نفسه

النص الأصلي

للبيع - 560 GB - بيانات مدنية حديثة بالكامل من 2 يناير 2026 - الدول المشمولة: السعودية مصر قطر دول أوروبية الولايات المتحدة - المحتويات: بيانات أفراد - سجلات خاصة - مستندات شخصية - صور - معلومات بنوك وشركات

ما يمكن إثباته — العرض والحجم المزعوم والأسواق الخمس المذكورة.

ما لم يثبت — أي بيانات قطرية يحتويها الملف إن وُجدت، أو مصدره.

بطاقة الدليل B16 | 22 يوليو 2026

Security news relay

قناة ناقلة على Telegram لإدراج في منتدى · Telegram · الإنجليزية

النص الأصلي

```
[About 30,000] Medical Professionals' CVs Leaked from [private hospital] [...] containing [about 31,000] CV files belonging to healthcare professionals. [file-format counts removed]
```

الترجمة

> تسريب السير الذاتية لـ [نحو 30,000] من المهنيين الطبيين من [مستشفى خاص] [...] تحتوي على [نحو 31,000] ملف سيرة ذاتية تعود لمهنيين في الرعاية الصحية. [أُزيلت أعداد الملفات حسب الصيغة]

ما يمكن إثباته	أن قناة ناقلة وصفت إدراجًا لملفات سير ذاتية لموظفين منسوبًا إلى المستشفى.
ما لم يثبت	الإدراج نفسه أو الملفات أو مصدرها.

عروض أصغر للهويات وبيانات الاعتماد. إلى جانب الادعاءات الستة عشر، رصدنا عروضًا أضيق تشير إلى الاتجاه نفسه. لم يُتحقق من أي منها.

التاريخ	العرض المرصود	قراءتنا
يناير–فبراير	قوائم بيانات اعتماد موسومة بنطاق حكومي وبنطاق اتصالات قطري (نحو 9,000 سطر في منتدى واحد)	إعادة تدوير نموذجية لقوائم الدمج (combolist)؛ والمصدر المرجح هو أجهزة المستخدمين وكلمات المرور المعاد استخدامها، لا الأنظمة نفسها
مارس	بائع يعلن عن "Qatar RAT 2026" في منتدى لبطاقات الدفع المسروقة	بيع برمجية خبيثة بوسم دولة؛ دون تسمية هدف
أبريل	صور جوازات سفر مع بيانات اتصال لـ 13 دولة، من بينها قطر	مواد هوية لاحتيال KYC؛ المصدر غير معروف
يونيو–يوليو	رفع آلي في منتديات لقاعدة بيانات موقع توظيف و"سجلات قطر"	عمليات رفع بواسطة روبوتات؛ الحجم والعمر غير معروفين

التاريخ	العرض المرصود	قراءتنا
يوليو	قائمة دمج (combolist) من 4,000 سطر موسومة بنطاقات تعليمية قطرية	قد تدعم إعادة استخدام بيانات الاعتماد ضد أنظمة الجامعات
أكتوبر	قاعدة بيانات بائع تجزئة إقليمي "للسعودية والكويت وقطر"، 27 مليون صف	من بين عملاء بائع تجزئة أجنبي مقيمون في قطر

4.5 دراسات حالة

تعرض كل حالة الادعاء، وما يمكننا إثباته، واستجابة متناسبة، مع التسلسل الزمني والبدائل والحدود حيثما توافرت.

A

الحالة A

ناشران يدّعيان استهداف شركة قطاع الطاقة نفسها

بطاقة الدليل B01 | 19 فبراير 2026 | منتدى تسريبات | الطاقة

ادعاءان، غير متحقق منهما

الادعاء	في 19 فبراير وصف منشور في منتدى اختراقات وصولًا إلى السحابة ودليل الهوية وأنظمة أمن المباني لدى شركة قطرية في قطاع الطاقة، مع سجلات للموظفين. وقبل ذلك بيوم نقلت أداة رصد عامة ادعاءً مشابهًا، نسبته إلى شخصية تُدعى Montaro.
التسلسل الزمني	في 10 مارس ادّعى ناشر ثانٍ، *ELIPHAS SYNDICATE*، امتلاك تفريغ لقاعدة بيانات الشركة نفسها، يضم سجلات للموظفين، وقال إنه مسح خادمًا.
ما يمكننا إثباته	أن ناشرين قدّما ادعاءات متداخلة بفارق ثلاثة أسابيع وبأحجام مختلفة، وأن كلا المنشورين يتضمن حقولًا من نوع بيانات الموظفين. لا تثبت المنشورات وجود وصول أو سرقة بيانات أو أي عملية مسح.
البدائل	جهة واحدة تستخدم اسمين؛ ناشر ثانٍ ينسخ الأول؛ بيانات موارد بشرية أو متعاقدين معاد تدويرها؛ بيانات مأخوذة من مورّد.
الحدود	لم تُقيَّم أي عيّنة، ولم نعثر على أي بيان رسمي أو بيان من الشركة حتى تاريخ القطع.
الاستجابة	مراجعة أدوار الدليل ذات الامتيازات، ومفاتيح السحابة المخزنة في إعدادات التطبيقات، والحسابات على أنظمة أمن المباني. والتحقق من وصول المورّدين إلى الأنظمة نفسها.
الخلاصة	**ذكر ناشران الشركة نفسها: راجعوا الأدوار ذات الصلاحيات المميزة ووصول الموردين قبل أن يتحدث أحد عن اختراق.**

B

الحالة B

عرض بيانات أفراد جهة أمنية حكومية

بطاقة الدليل B03 | 10 مارس 2026 | منتدى تسريبات | الحكومة (الأمن)

ادعاء غير متحقق منه

الادعاء	في 10 مارس عرضت شخصية نسجّلها باسم *TheAshborn* بيانات أفراد عن 1,900 عضو في جهة أمنية حكومية مقابل 10,000 USD، مع لقطتي شاشة.
ما يمكننا إثباته	العرض، والحقول المزعومة (الأسماء وأرقام الاتصال والمسميات الوظيفية والإدارات والجنسية)، ونسختان في منتديين في اليوم نفسه. ونقلته قناة Telegram في اليوم نفسه.
البدائل	دليل موظفين مصدَّر من نظام طرف ثالث؛ قائمة اتصال أقدم؛ اختراق حقيقي.
الاستجابة	مقارنة الحقول المزعومة بصادرات الدليل والموارد البشرية. وتحذير الموظفين من التصيّد الموجّه وانتحال الهوية، لأن بيانات الاتصال الخاصة بأفراد الأمن مفيدة لكليهما.
الخلاصة	**أيًا كان مصدرها، فإن بيانات الاتصال بالموظفين تدعم التصيد الموجّه: نبّهوا الموظفين وقارنوا الحقول بصادرات الدليل.**

C

الحالة C

المصرف الكبير نفسه يُدّعى استهدافه مرتين

ادعاء غير متحقق منه (متكرر)

بطاقة الدليل B04 | 10 نوفمبر 2026 | منتدى تسريبات

القطاع المصرفي

الادعاء	في 10 و 14 نوفمبر عرض بائعون في منتديي اختراقات عددًا كبيرًا جدًا من سجلات العملاء وسجلات للموظفين منسوبة إلى مصرف قطري كبير. وكان السعر المطلوب USD 1,500، أو USD 900 للنصف.
التسلسل الزمني	في أبريل عرض موضوع في منتدى بيانات موظفين وتحويلات ومستخدمين منسوبة إلى المصرف نفسه. وفي أغسطس وصفت قناة ناقلة على Telegram إدراجًا في منتدى يُقال إنه يمتد على 2024–2026. لم نعثر على بيان من المصرف أو السلطات يؤكد ذلك حتى تاريخ القطع.
ما يمكننا إثباته	أن العروض تسمّي المصرف، وتدرج مخططًا لسجلات العملاء يتضمن حقلًا لرقم البطاقة، وتتكرر عبر منصات مختلفة. ولا تثبت مصدر الملف أو عمره أو حدوث عملية بيع.
البدائل	بيانات مجمّعة أو أقدم أُعيد تقديمها على أنها جديدة؛ بيانات من شريك أو معالج بطاقات؛ اختراق حقيقي.
الاستجابة	مقارنة المخطط المزعوم بصادرات النظام المصرفي الأساسي ونظام البطاقات. ومراقبة التصيّد الموجّه إلى العملاء الذي يقتبس تفاصيل الحسابات، وإعداد إشعار للعملاء تحسبًا للتحقق من عيّنة.

الخلاصة

ادعاء متكرر يتضمن مخططه حقلًا لرقم البطاقة: قارنوا بالصادرات وجهّزوا رسائل العملاء.

D

الحالة D

مجموعة مدارس خاصة

ادعاء غير متحقق منه

بطاقة الدليل B06 | 8 يونيو 2026 | منتدى تسريبات | التعليم

الادعاء	في 8 يونيو قال ناشر في منتدى إنه سيطر على أنظمة مجموعة مدارس خاصة، واستخرج أكثر من 100 GB وحذف قواعد البيانات. وأدرج جوازات سفر وبطاقات هوية وسجلات موظفين وعناوين سكن.
ما يمكننا إثباته	المنشور، وأنواع البيانات المزعومة، وقائمة بأسماء قواعد البيانات. لم نعثر على بيان من المدرسة أو من أي سلطة.
البدائل	مبالغة في اختراق أصغر لموقع إلكتروني؛ بيانات من مزوّد برمجيات لإدارة المدارس.
الاستجابة	ينبغي للمدارس التحقق من النسخ الاحتياطية وحسابات استضافة المواقع ووصول مزوّدي البرمجيات، ومعاملة بيانات هوية أولياء الأمور والأطفال أولويةً في الإخطار إذا تأكدت عيّنة.
الخلاصة	**بيانات هوية الأطفال ترفع حجم المخاطر: راجعوا النسخ الاحتياطية ووصول مزودي الخدمة، وجهّزوا الإخطار.**

E

الحالة E

رموز تطبيقات في عيّنة منسوبة إلى جهة في القطاع العام

نُشرت عينة

بطاقة الدليل B07 | 3 سبتمبر 2026 | منتدى | القطاع العام

الادعاء	في 3 سبتمبر قال منشور في منتدى إن جهة قطرية في القطاع العام تعرضت للاختراق. ونشر عيّنة قصيرة مما يبدو أنه رموز وصول إلى التطبيقات وصفوف مستخدمين.
ما يمكننا إثباته	بنية العيّنة. الرموز المنشورة في منشور عام تمثل خطرًا سواء صحّ الادعاء الأوسع أم لا، لأن أي شخص يستطيع تجربتها.
الاستجابة	تدوير أي رموز ومفاتيح مكشوفة، وقصر الخدمة المكشوفة على شبكات معروفة، ومراجعة سجلات الوصول بدءًا من التواريخ الواردة في العيّنة.
الخلاصة	**بدّلوا الرموز المكشوفة الآن؛ فالرمز المنشور علنًا خطر سواء صحّ ادعاء الاختراق أم لا.**

F

الحالة F

مشترون يطلبون الوصول إلى شبكات حكومية

طلب مرصود (منشوران)

بطاقة الدليل B08 | 3 سبتمبر 2026

منتدى، مع النص نفسه على Telegram | الحكومة

الادعاء	في 3 سبتمبر نشر مستخدم في منتدى ومستخدم على Telegram الطلب نفسه: وصول عبر سطح المكتب البعيد أو VPN أو إلى قواعد بيانات لدى جهات حكومية في قطر ودولتين أخريين في المنطقة. وسمّى طلب مشابه في أبريل اثنتي عشرة دولة تقريبًا.
ما يمكننا إثباته	وجود طلب على الوصول، لا الوصول نفسه.
لماذا يهم	الطلب من هذا النوع هو ما يحوّل سجلات برامج سرقة المعلومات والخدمات البعيدة المكشوفة إلى عمليات اختراق.
الاستجابة	مراقبة عمليات تسجيل الدخول الحكومية عبر VPN وسطح المكتب البعيد بحثًا عن أجهزة جديدة وساعات غير معتادة. وإعطاء الأولوية لارتباطات أجهزة الموظفين الواردة في الفصل 3.
الخلاصة	**يريد المشترون وصولًا عن بُعد إلى جهات حكومية: راقبوا عمليات تسجيل الدخول عبر VPN وسطح المكتب البعيد وتحققوا من أجهزة الموظفين.**

بطاقة الدليل B04 — 10 نوفمبر 2026

UNC6783 (self-applied channel name)

منتدى تسريبات · Forum · الإنجليزية

النص الأصلي

```
a leak occurred targeting one of the Banks in Qatar in large amounts [[...] customer data, and [...] employees in several branches of [large bank] in 2026.] [...] Data include [...] CUSTOMERID, SEX, NAME, TYPE [...] ADDRESS [...] MOBILENUMBER, ATMCARDNUMBER [samples removed]
```

الترجمة

وقع تسريب استهدف أحد البنوك في قطر بكميات كبيرة [[...] من بيانات العملاء، و[...] موظفين في عدة فروع لـ[بنك كبير] في 2026.] [...] تشمل البيانات [...] CUSTOMERID, SEX, NAME, TYPE [...] ADDRESS [...] MOBILENUMBER, ATMCARDNUMBER [تمت إزالة العينات]

ما يمكن إثباته

الادعاء والمخطط المزعوم للبيانات وعرض شبه مطابق على منتدى ثانٍ بعد أربعة أيام بسعر 1,500 USD.

ما لم يثبت

مصدر الملف أو عمره، أو أي عملية بيع، أو اختراق للبنك.

بطاقة الدليل B05 — 26 أغسطس 2026

Security news relay

قناة ناقلة على Telegram لإدراج في منتدى · Telegram · الإنجليزية

النص الأصلي

```
[large bank] Data Offered on Underground Forum. A hacker is advertising a database originating from [large bank] sources, with the listing referencing data spanning 2024-2026. [...] User data, Transaction data [...] Government-related records, Defence-related records
```

الترجمة

بيانات [بنك كبير] معروضة في منتدى سري. يعلن أحد المخترقين عن قاعدة بيانات مصدرها [بنك كبير]، ويشير الإدراج إلى بيانات تمتد من 2024-2026. [...] بيانات المستخدمين، بيانات المعاملات [...] سجلات متعلقة بالحكومة، سجلات متعلقة بالدفاع

ما يمكن إثباته

أن قناة ناقلة وصفت إدراجًا في منتدى منسوبًا إلى البنك في أغسطس.

ما لم يثبت

الإدراج نفسه أو محتوياته أو أي صلة بعرض نوفمبر.

بطاقة الدليل B06 — 8 يونيو 2026

Unnamed poster — منتدى تسريبات · Forum · الإنجليزية

النص الأصلي

```
[private school group] in Qatar was
hacked, and all databases and domains
were compromised. After extracting
the data, we deleted all databases
and took the website offline. The
data obtained included passports, ID
cards, full names [...] The total
amount of data obtained exceeded 100
gigabytes. [sample link removed] To
purchase all data, please contact us
[contact removed]
```

الترجمة

تم اختراق [مجموعة مدارس خاصة] في قطر، واختُرقت جميع قواعد البيانات والنطاقات. بعد استخراج البيانات، حذفنا جميع قواعد البيانات وأخرجنا الموقع عن الخدمة. شملت البيانات التي حصلنا عليها جوازات السفر وبطاقات الهوية والأسماء الكاملة [...] تجاوز إجمالي البيانات التي حصلنا عليها 100 غيغابايت. [تمت إزالة رابط العينة] لشراء جميع البيانات، يرجى التواصل معنا [تمت إزالة وسيلة الاتصال]

ما يمكن إثباته	الادعاء وأنواع البيانات المزعومة وأسماء قواعد البيانات المدرجة.
ما لم يثبت	أي حذف أو انقطاع أو سرقة بيانات؛ لم نجد أي بيان من المدرسة أو من جهة رسمية.

بطاقة الدليل B07 — 3 سبتمبر 2026

Unnamed poster — منتدى · Forum · الإنجليزية

النص الأصلي

```
[public-sector body] breached.
[address removed] Sample:
ID,Name,Token,Status,Expire At [...]
[tokens removed]
```

الترجمة

اختراق [جهة في القطاع العام]. [تمت إزالة العنوان] عينة: ID,Name,Token,Status,Expire At [...] [تمت إزالة الرموز المميزة]

ما يمكن إثباته	عينة تبدو صفوفها كرموز وصول لتطبيق وسجلات مستخدمين.
ما لم يثبت	ما إذا كانت الرموز صالحة أو ما إذا كان ادعاء الاختراق الأوسع صحيحًا.

بطاقة الدليل B08 — 3 سبتمبر 2026

Anonymous buyer منتدى، مع النص نفسه على Telegram · Forum · الإنجليزية

النص الأصلي

```
hi I look for RDP, VPN Or Any Network Access in any GOV organs in Qatar, Jordan And Saudi Arabia Or Any Leaked Secret Data Bases From There Networks. Any Things You Have for Sale?
```

الترجمة

مرحبًا، أبحث عن RDP أو VPN أو أي وصول إلى شبكة في أي جهة حكومية في قطر والأردن والسعودية، أو أي قواعد بيانات سرية مسربة من شبكاتها. هل لديكم أي شيء للبيع؟

ما يمكن إثباته: طلب للوصول إلى شبكات حكومية في ثلاث دول، نُشر مرتين في اليوم نفسه.

ما لم يثبت: أن أحدًا وفّر هذا الوصول.

بطاقة الدليل B18 — 16 مايو 2026

Unnamed poster منتدى · Forum · الإنجليزية

النص الأصلي

```
DATABASE [Qatar] [consumer discount app] [about 300k] users data, format: csv fields: id, full_name, mobile, email, password [...] dob, nationality, residence [...] Sample: [removed]
```

الترجمة

قاعدة بيانات [قطر] [تطبيق خصومات للمستهلكين] بيانات [نحو 300k] مستخدم، الصيغة: csv الحقول: id, full_name, mobile, email, password [...] dob, nationality, residence [...] عينة: [تمت إزالتها]

ما يمكن إثباته: العرض والحقول؛ وتصف قنوات ناقلة في يناير ومارس الملف نفسه، وتؤرخ إحداها الاختراق في 2023.

ما لم يثبت: عمر الملف أو مصدره، أو أي انكشاف حالي.

4.6 ما تضيفه المنتديات

لم تُسهم المنتديات إلا بـ 90 منشورًا موسومًا و 334 منشورًا آخر يذكر قطر خلال العام، لكنها تحمل معظم الادعاءات المحددة الواردة أعلاه. ومعظم نتائج المنتديات الأخرى صفحات بريد مزعج لمحركات البحث وقوائم عملاء محتملين متعددة الدول. كما نشر مشترون في المنتديات طلبات للوصول إلى جهات حكومية قطرية (الحالة F). والطلب على الوصول إلى جهات قطرية وعلى بيانات الهوية القطرية هو في حد ذاته نتيجة.

الخلاصات الرئيسية

01 تهيمن على الحجم الخام منشورات آلية باللغة التركية؛ اقرأ الأعداد المنقّحة فقط، وتعامل معها على أنها حد أعلى.

02 تتركز الادعاءات المحددة على الطاقة والمصارف والأمن والتعليم والقطاع العام؛ ولم يتأكد أي منها حتى تاريخ القطع.

03 تكرار تسمية المؤسسة نفسها سبب للتحقق السريع، لا دليل على وقوع اختراق.

الفصل 5

أمثلة على الاستهداف بحسب القطاع

يجيب هذا الفصل عن

أي القطاعات القطرية تُذكر في المنشورات الإجرامية والسياسية، وما نوع الاستجابة التي يحتاجها كل منها؟

10

قطاعات رُصد فيها نشاط، من الحكومة إلى التجزئة

باختصار

تُظهر المنشورات أدناه كيف تتحدث الجهات الإجرامية والسياسية عن المؤسسات القطرية. تسمّي الجهات السياسية مواقع إلكترونية حكومية وتدّعي تعطيلها. ويسمّي البائعون الإجراميون جهات توظيف كبرى وحائزي بيانات، أو يدرجون قطر سوقًا واحدة بين أسواق كثيرة. وتضيف التقارير الرسمية وأبحاث المورّدين التجسس والاحتيال. تحقق من كل ادعاء مع المؤسسة التي يسمّيها، وابدأ بالاستجابة الأولى الخاصة بالقطاع.

يُوصف الضحايا بحسب دورهم وفق السياسة الواردة في **الملحق A.9**. والأمثلة مأخوذة من منشورات Blackhole والمصادر العامة في الملحق C.

الحكومة

ادعاء DDoS، ادعاء بيانات، طلب وصول، تجسس

مثال على النشاط المرصود (مجهّل الهوية)

ادعاءات DDoS ضد بوابات حكومية والوزارات وجهة تنظيمية مالية (مارس؛ الفصل 6)؛ عرض بيانات أفراد جهة أمنية حكومية (مارس)؛ رموز عيّنة منسوبة إلى جهة في القطاع العام (سبتمبر)؛ مشترون يطلبون وصولًا حكوميًا عبر VPN وسطح المكتب البعيد (أبريل، سبتمبر)؛ تجسس مرتبط بالصين ضد أهداف حكومية وأهداف في الطاقة (أبحاث مورّدين، مارس)

ما يعنيه

ادعاءات التوافر كثيرة الضجيج؛ أما المخاطر الجوهرية فهي بيانات الموظفين ورموز التطبيقات المكشوفة والوصول عن بُعد

الاستجابة الأولى

الاتفاق مسبقًا على بيانات الحالة؛ تدوير الرموز المكشوفة؛ مراقبة عمليات تسجيل الدخول عبر VPN

الطاقة

ادعاءات وصول وبيانات، إدراج لدى مجموعة فدية، ادعاء DDoS، تجسس

مثال على النشاط المرصود (مجهّل الهوية)

ناشران ادّعيا استهداف شركة قطاع الطاقة نفسها (فبراير، مارس؛ الحالة A)؛ مجموعة ادّعت الحصول على قاعدة بيانات مقاول هندسي (فبراير)؛ متعاقد في خدمات النفط أدرجته مجموعة ابتزاز (يوليو؛ خارج عدد Ransompedia)؛ موقع في قطاع الطاقة على قائمة DDoS لمواقع طاقة إقليمية (مارس)؛ طُعوم عن ضربات على منشآت النفط والغاز (أبحاث مورّدين، مارس)

ما يعنيه

أنظمة الهوية والمورّدين وأمن المباني هي المسارات المزعومة؛ والمتعاقدون جزء من التعرّض

الاستجابة الأولى

مراجعة الأدوار ذات الامتيازات ووصول المورّدين؛ البحث عن طُعوم الأرشيفات والاختصارات

المصارف

ادعاء بيانات، بطاقات دفع مسروقة، تداول حسابات، ادعاء DDoS

مثال على النشاط المرصود (مجهّل الهوية)

مصرف كبير سُمّي في عرض لسجلات عملاء (نوفمبر؛ الحالة C) وفي عروض سابقة (أبريل، أغسطس)؛ عرض "قاعدة بيانات" منسوبة إلى جهة في القطاع المالي (يناير)؛ مخرجات أدوات فحص بطاقات تسمّي سبع جهات إصدار قطرية؛ بيع حسابات تداول مسجلة في قطر؛ جهة تنظيمية مالية على قائمة DDoS (مارس)

ما يعنيه

معظم المنشورات أدوات احتيال؛ والإشارات الأولى التي ينبغي التحرك بشأنها هي الإدراجات الحالية لبيانات الاعتماد، ثم أجهزة الموظفين (الفصل 9)

الاستجابة الأولى

فرز الإدراجات الحالية لبيانات الاعتماد؛ مقارنة المخططات المزعومة بالصادرات؛ التنبيه على حالات الرفض الصادرة عن أدوات الفحص

الاتصالات

إدراج لدى مجموعة فدية، قائمة دمج (combolist)، DDoS

مثال على النشاط المرصود (مجهّل الهوية)

شركة بنية تحتية للاتصالات أدرجتها مجموعة ابتزاز (مايو)؛ قوائم بيانات اعتماد موسومة بنطاق اتصالات (فبراير)؛ وقع معظم DDoS المقاس على شركات الاتصالات

ما يعنيه

تمتص شركات الاتصالات معظم DDoS المقاس؛ وتتداول بيانات اعتماد العملاء في قوائم معاد تدويرها

الاستجابة الأولى

التأكد من سعة التصدي لـ DDoS لدى المزوّد الأعلى؛ فرض إعادة تعيين كلمات المرور لحسابات العملاء المدرجة

الطيران والنقل

ادعاء بيانات، إعادة بيع حسابات

مثال على النشاط المرصود (مجهّل الهوية)

جهة في قطاع الطيران سُمّيت في عرض "قاعدة بيانات" (مارس، غير متحقق منه)؛ حسابات ولاء لشركة طيران خليجية في متاجر الأميال على مدار العام

ما يعنيه

الاستيلاء على حسابات الولاء والبريد الإلكتروني هو مسار الاحتيال المرصود، لا اختراق شركة الطيران

الاستجابة الأولى

إضافة MFA إلى حسابات الولاء؛ مراقبة الشذوذ في عمليات الاسترداد

التعليم

ادعاء بيانات، إدراج لدى مجموعة فدية، قائمة دمج (combolist)

مثال على النشاط المرصود (مجهّل الهوية)

ادعاء ضد مجموعة مدارس خاصة (يونيو؛ الحالة D)؛ معهد بحثي أدرجته مجموعة ابتزاز (أبريل)؛ قائمة دمج (combolist) لنطاقات تعليمية (يوليو)

ما يعنيه

تتعلق الادعاءات ببيانات هوية الأطفال وأولياء الأمور وبأنظمة البحث؛ ولم يُؤكَّد أي منها

الاستجابة الأولى

التحقق من النسخ الاحتياطية ووصول مزوّدي البرمجيات؛ فرض MFA على الموظفين

الإعلام

برنامج تجسس (نتيجة Citizen Lab)

مثال على النشاط المرصود (مجهّل الهوية)

استُهدف 45 جهازًا على الأقل لدى Al Jazeera ببرنامج التجسس التجاري Candiru في 2024 و2025 عبر الإعلانات الموجّهة، وأُصيبت أجهزة منها (Citizen Lab، أكتوبر؛ الفصل 7)

ما يعنيه

قد تُستهدف أجهزة المؤسسات الإعلامية ببرامج تجسس تجارية

الاستجابة الأولى

تحديث أجهزة الموظفين باستمرار؛ التعامل مع عمليات إعادة التوجيه غير المعتادة الناتجة عن الإعلانات بوصفها مؤشرًا على حادث

الرعاية الصحية

ادعاءات بيانات

مثال على النشاط المرصود (مجهّل الهوية)

سجلات مرضى وتأمين (مايو) وملفات سير ذاتية لكوادر طبية (يوليو) منسوبة إلى مستشفى خاص

ما يعنيه

تحمل سجلات المرضى وملفات التوظيف وثائق هوية

الاستجابة الأولى

مراجعة صادرات منصات التوظيف ومدة الاحتفاظ بها

التجزئة والمستهلكون

ادعاءات بيانات، معاد تدويرها في معظمها

مثال على النشاط المرصود (مجهّل الهوية)

إعادة عرض ملف نحو 300,000 مستخدم لتطبيق خصومات (يناير–مايو)؛ "بيانات تسوّق قطر" (يوليو)؛ قاعدة بيانات بائع تجزئة إقليمي تسمّي قطر (أكتوبر)

ما يعنيه

بيانات المستهلكين القديمة تغذّي التصيّد والاستيلاء على الحسابات

الاستجابة الأولى

فرض إعادة تعيين كلمات المرور حيث يتأكد التطابق

الخدمات المهنية والإنشاءات

إدراجات لدى مجموعات فدية

مثال على النشاط المرصود (مجهّل الهوية)

مكتب محاماة وعدة متعاقدين أدرجتهم مجموعات ابتزاز (أبريل–نوفمبر)

ما يعنيه

تسمّي الإدراجات شركات متوسطة الحجم لا علامات تجارية كبرى

الاستجابة الأولى

اختبار عمليات الاستعادة؛ مراجعة الوصول عن بُعد للمورّدين

قراءة عبر القطاعات. تنقسم الادعاءات الخاصة بمؤسسات بعينها إلى مجموعتين. تسمّي الجهات السياسية مواقع إلكترونية حكومية وتدّعي تعطيلها. وتسمّي الجهات الإجرامية جهات توظيف كبرى وحائزي بيانات، أو تعامل قطر سوقًا واحدة بين أسواق كثيرة. أما التجسس، الذي يرصده المورّدون، فيستهدف الحكومة والطاقة ولم يظهر في بيانات مواقع التسريب والمنتديات التي بحثنا فيها.

الخلاصات الرئيسية

01

تسمّي الجهات السياسية مواقع حكومية؛ ويسمّي البائعون الإجراميون جهات توظيف كبرى وحائزي بيانات.

02

يواجه قطاع الطاقة ادعاءات بيانات وطُعوم تجسس معًا، ويظهر متعاقدوه في إدراجات الابتزاز.

03

بالنسبة إلى المصارف وشركات الطيران، يمر مسار الاحتيال المرصود عبر حسابات العملاء والبريد الإلكتروني والولاء.

الفصل 6

نشاط القرصنة الناشطة (الهاكتفيزم) وهجمات DDoS

يجيب هذا الفصل عن

من ادّعى تنفيذ هجمات على قطر في 2026، وماذا أظهرت القياسات والتقارير، وكيف ينبغي للمؤسسة أن تستعد للموجة التالية؟

31,836

هجمات DDoS على قطر رصدتها NETSCOUT في الفترة يناير-يونيو 2026

في هذا الفصل

6.1 التسلسل الزمني

6.2 موجة مارس: الادعاءات في مقابل القياس

6.3 ادعاءات أخرى بكلمات أصحابها

6.4 دروس للمدافعين

باختصار

تركّزت ادعاءات الهاكتفيست ضد قطر بين 28 فبراير و 25 مارس 2026، بعد بدء التصعيد الإقليمي. ادّعت أربع مجموعات تنفيذ هجمات DDoS على بوابات حكومية ووزارات وبوابة فوترة ودفع لخدمة عامة وجهة تنظيمية مالية وموقع في قطاع الطاقة. لم نعثر على أي بيان رسمي يؤكد حدوث انقطاع. كانت حركة DDoS المقاسة مرتفعة، وصنّفت NETSCOUT معظم الأهداف على أنها مشغلو اتصالات؛ ولا تُظهر بياناتها ما إذا كانت المواقع المسمّاة قد أُصيبت. تعاقدوا على خدمة تخفيف الهجمات لدى مزوّد المنبع، واتفقوا مسبقاً على الجهة التي تؤكد حالة الخدمة قبل الموجة التالية.

6.1 التسلسل الزمني

28 فبراير 2026

تقرير الوضع من CloudSEK

يسجّل هجوم DDoS أعلنت عنه BD Anonymous Team بنفسها على خدمة إلكترونية تابعة لإحدى الوزارات، 28 فبراير-1 مارس

28 فبراير 2026

تقرير الوضع من CloudSEK

يسجّل هجوم DDoS ادّعته DieNet على بوابات حكومية ومشغّلي اتصالات ومطارات ومصارف في ست دول، من بينها قطر

3 مـارس 2026

Keymous Plus

تدّعي تعطيل بوابة فوترة ودفع لخدمة عامة، مع رابط فحص التوافر

6 مـارس 2026

قناة ناقلة لـ DieNet

تسعة منشورات آلية تذكر مواقع حكومية قطرية بوصفها "مستهدفة حالياً"

9 مـارس 2026

Intel 471

تضع قطر ضمن المواقع العشرة الأكثر ورودًا في الادعاءات للأسبوع الذي بدأ في 27 فبراير

12 مـارس 2026

Keymous Plus

تدرج 13 موقعاً حكومياً، من بينها بوابات ووزارات وجهة تنظيمية مالية

14 مـارس 2026

Team 313

تدّعي أن بوابة حكومية "عُطّلت بالكامل" لمدة ساعة؛ وتمدّد الادعاء في 15 مارس

24 مـارس 2026

وزارة الداخلية

تحذّر من اتصالات ورسائل "تستغل الوضع الراهن" للحصول على البيانات المصرفية ورموز التحقق لمرة واحدة

24 مـارس 2026

Keymous Plus

"زيارة اختبارية" ضد خمس وزارات؛ وتقول إن بعض المواقع عادت للعمل

25 مـارس 2026

Keymous Plus

تذكر موقعاً في قطاع الطاقة ضمن 12 موقعاً إقليمياً في قطاع الطاقة

10 أبـريـل 2026

The National

تفيد بادعاءات مبكرة ضد مواقع في قطاع الطاقة والإعلام، ثم بتراجع في نشاط القرصنة الناشطة المباشر

19 يـونـيـو 2026

BD Anonymous Team

تدّعي إسقاط الموقع الإلكتروني لقوة أمنية، مستشهدة بوجود عسكري أجنبي

العلامات الداكنة هي منشورات الجهات الفاعلة، والعلامات المفرغة هي القنوات الناقلة وتقارير الأطراف الثالثة، والعلامات المرجانية هي البيانات الرسمية. التواريخ هي تواريخ النشر بتوقيت UTC؛ وتوقيت الدوحة هو UTC+3. يتعلق تحذير وزارة الداخلية بالاحتيال لا بهجمات DDoS؛ وهو البيان الرسمي الوحيد المرتبط بالتصعيد الذي عثرنا عليه.

6.2 موجة مارس: الادعاءات في مقابل القياس

الادعاءات. بين 28 فبراير و 25 مارس ادّعت أربع مجموعات تنفيذ هجمات DDoS على أهداف قطرية. نشرت Keymous Plus أربع قوائم تذكر بوابة فوترة ودفع لخدمة عامة و 13 موقعاً حكومياً وخمس وزارات وموقعاً في قطاع الطاقة [S2]. ونشرت قناة ناقلة تسعة منشورات آلية لـ DieNet في 6 مارس، يذكر كل منها موقعاً حكومياً مع نتيجة فحص التوافر [S34]. وادّعت Team 313 استهداف بوابة حكومية في 14 و 15 مارس. وسجّلت CloudSEK ادعاءً لـ BD Anonymous Team ضد خدمة إلكترونية تابعة لإحدى الوزارات [S29].

بطاقة الدليل B10 — 12 مارس 2026

Keymous Plus قناة الجهة الفاعلة · Telegram

· الإنجليزية، كما نُشرت

النص الأصلي

```
A visit been planned to be back on
the heat [...] Qatar: [state body]
Check Host [government portal] Check
Host [ministry] Check Host [ministry]
Check Host [...] [financial
regulator] Check Host [links removed]
```

الترجمة

زيارة مخططة للعودة إلى النشاط [...] قطر: [جهة حكومية] Check Host [بوابة حكومية] Check Host [وزارة] Check Host [وزارة] Check Host [...] [جهة تنظيمية مالية] Check Host [تمت إزالة الروابط]

ما يمكن إثباته	قائمة تضم 13 موقعًا حكوميًا قطريًا مع روابط فحص التوافر، تليها مواقع في دولة أخرى.
ما لم يثبت	أي انقطاع أو أثر.

بطاقة الدليل B11 — 14 مارس 2026

Team 313 قناة الجهة الفاعلة · Telegram

· العربية، مع نص إنجليزي من المجموعة نفسها

النص الأصلي

نفذت [...] فريق 313 هجوم سيبراني استهدف [بوابة حكومية] حيث ادى الهجوم لتعطيل الموقع الالكتروني بالكامل. سيستمر الهجوم لمدة ساعة واحدة.

ما يمكن إثباته	الادعاء ورابط فحص وتحديث في اليوم التالي يزعم عدة ساعات إضافية.
ما لم يثبت	انقطاع الخدمة؛ لم يُعثر على أي بيان رسمي أو من المؤسسة المعنية.

الرواية الرسمية. لم نعثر على أي بيان من جهة قطرية رسمية أو من مؤسسة مسمّاة يؤكد حدوث انقطاع بسبب هجوم DDoS خلال هذه الفترة. حذّرت وزارة الداخلية في 24 مارس من احتيال يستغل "الوضع الراهن" [S35]. ويتعلق هذا التحذير باتصالات ورسائل التصيّد الاحتيالي، لا بتوافر الخدمات.

القياس. سجّلت NETSCOUT عدد 31,836 هجوم DDoS على قطر في الفترة يناير–يونيو 2026، بمتوسط مدة بلغ 20.97 دقيقة. واستقبل مشغّلو الاتصالات السلكية 29,808 منها، وكان تضخيم DNS أكثر الأساليب شيوعاً [S32]. وأفادت StormWall بأن الهجمات على قطر ارتفعت بنسبة 75% على أساس سنوي في الربع الأول، وبأن حصة قطر من هجمات DDoS الإقليمية ارتفعت من 8% إلى 14% [S31].

ما يمكننا إثباته. تصف الادعاءات وبيانات القياس عن بُعد أموراً مختلفة. فبيانات القياس تحصي الهجمات على الشبكات، ومعظمها لدى مشغّلي الاتصالات، ولا تسمّي أي مجموعة. أما الادعاءات فتسمّي مواقع حكومية وتستند إلى روابط فحص التوافر. ولا يؤكد أيٌّ منهما حدوث انقطاع لدى مؤسسة مسمّاة، ولذلك لا نجمعهما في نسبة أو معدل نجاح.

النقطة	ادعاءات المجموعات	الرواية الرسمية	القياس والتقارير
التوقيت	28 فبراير–25 مارس، وادعاء إضافي واحد في يونيو [S2][S29]	لم يُعثر على بيان بشأن DDoS	قطر ضمن العشرة الأوائل الأسبوعية لدى Intel 471 بدءاً من 27 فبراير [S30]؛ والإفادة بتراجع بحلول أبريل [S33]
الأهداف	بوابات حكومية، ووزارات، وبوابة فوترة ودفع لخدمة عامة، وجهة تنظيمية مالية، وموقع في قطاع الطاقة [S2]	لم يُؤكَّد أي منها	29,808 من أصل 31,836 هجوماً مقاساً أصابت مشغّلي الاتصالات السلكية [S32]
الأثر	"عُطّلت بالكامل"، "متوقفة"، روابط فحص التوافر	غير مذكور	Intel 471: المجموعات "كثيراً ما تبالغ" في الأثر [S30]
الحجم	غير مذكور	غير مذكور	متوسط 20.97 دقيقة؛ وتضخيم DNS هو الأسلوب الأول [S32]
الأدوات	منشورات Keymous Plus و Team 313 تحمل كلتاهما روابط إحالة إلى العلامة التجارية نفسها لخدمة إغراق مأجورة (stresser) تجارية [S2]	غير مذكور	CloudSEK: الإسناد "معلن ذاتياً"، والتحقق التقني محدود [S29]
الإسناد	ادعاءاتها الخاصة	لا يوجد	تصف Unit 42 كلاً من Team 313 وDieNet بأنهما مجموعتان مواليتان لإيران [S28]

ماذا يعني ذلك. تزامنت موجة من ادعاءات هجمات DDoS مع التصعيد، وارتفعت الهجمات المقاسة. أما الانقطاعات المدّعاة في المواقع الحكومية فتبقى ادعاءات. وتُظهر روابط خدمة الإغراق المأجورة المشتركة أن مجموعتين على الأقل تروّجان للقدرة المستأجرة نفسها. وهذا يدعم وجود ارتباط بخدمة تجارية، لا وجود مشغّل مشترك.

6.3 ادعاءات أخرى بكلمات أصحابها

بطاقة الدليل B09 — 3 مارس 2026

Keymous Plus — قناة الجهة الفاعلة · Telegram · الإنجليزية، كما نُشرت

النص الأصلي

```
Lately [QA flag] [public-service provider]. Services for [service names], billing, and payment. Check Host [link removed] : 1000sec
```

الترجمة

مؤخرًا [علم قطر] [جهة خدمة عامة]. خدمات [أسماء الخدمات] والفوترة والدفع. Check Host [تمت إزالة الرابط] : 1000sec

ما يمكن إثباته — الادعاء ورابط فحص التوافر.

ما لم يثبت — انقطاع الخدمة؛ رابط الفحص يسجّل في أقصى الأحوال لحظة تعذّر وصول.

بطاقة الدليل B12 — 6 مارس 2026

DieNet (relayed) — قناة ناقلة لروبوت تتبع آلي · Telegram · الإنجليزية

النص الأصلي

```
DieNet network is currently targeting [government portal] and it may be down for you at the moment. Check-Host [...] Connection timed out [...] This is an automated [...]
```

الترجمة

شبكة DieNet تستهدف حاليًا [بوابة حكومية] وقد تكون متوقفة لديك في هذه اللحظة. Check-Host [...] انتهت مهلة الاتصال [...] هذه رسالة آلية [...]

ما يمكن إثباته — تسعة منشورات آلية في اليوم نفسه تذكر مواقع حكومية قطرية.

ما لم يثبت — من نفّذ الهجمات، أو أي انقطاع يتجاوز فحصًا انتهت مهلته.

بطاقة الدليل B15 — 24 مارس 2026

Keymous Plus قناة الجهة الفاعلة · Telegram

الإنجليزية، كما نُشرت

النص الأصلي

```
A testing visit. Qatar: [ministry]
Check Host [...] [ministry] [...]
[ministry] [...] [ministry] [...]
[ministry] [links removed] Some
websites still down others are up
after the test is down, Next visits
will be focusing on downtime.
```

الترجمة

زيارة اختبارية. قطر: [وزارة] Check Host [...] [وزارة] [...] [وزارة] [...] [وزارة] [...] [تمت إزالة الروابط] بعض المواقع لا تزال متوقفة وأخرى عادت للعمل بعد توقف الاختبار، والزيارات القادمة ستركز على التوقف.

ما يمكن إثباته	قائمة بخمس وزارات وتصريح المجموعة نفسها بأن بعض المواقع عادت للعمل.
ما لم يثبت	أي انقطاع أو مدته.

بطاقة الدليل B13 — 19 يونيو 2026

BD Anonymous Team قناة الجهة الفاعلة · Telegram

الإنجليزية، كما نُشرت

النص الأصلي

```
We have successfully took down The
Official site of [security force]
Cheakhost [link removed] [...]
[motive statement shortened] BD
Anonymous Team
```

الترجمة

نجحنا في إسقاط الموقع الرسمي لـ[قوة أمنية] Cheakhost [تمت إزالة الرابط] [...] [تم اختصار بيان الدافع] BD Anonymous Team

ما يمكن إثباته	الادعاء ورابط فحص؛ يذكر المنشور وجودًا عسكريًا أجنبيًا دافعًا له.
ما لم يثبت	انقطاع الخدمة؛ لم يُعثر على تقارير عامة بشأن هذا الادعاء.

لا يُحتسب ضمن نشاط الهاكتفيست. في 30 أكتوبر أفادت قناة ناقلة لأخبار الأمن بأن موقعًا إلكترونيًا في قطاع الطيران تعطل نحو 24 ساعة، ووسمت ذلك بأنه هجوم سيبراني. لم تتبنَّ أي مجموعة ذلك ولم نعثر على تفسير رسمي، لذلك لا نحتسبه.

ذكر ادعاء BD Anonymous Team في يونيو الموقع الإلكتروني لقوة أمنية، واستشهد بوجود عسكري أجنبي دافعاً له. ننقل الدافع المعلن بوصفه دافع المجموعة نفسها ولا نتخذ موقفاً منه. ولم نعثر على تقارير علنية عن هذا الادعاء.

6.4 دروس للمدافعين

1. **اتفقوا مسبقاً على الخطاب العام.** نادراً ما تقيس لقطة الشاشة التي تنشرها مجموعة وبيانات القياس لدى مشغّل الاتصالات الشيء نفسه. حدّدوا مسبقاً من يؤكد حالة الخدمة، وفي غضون أي مدة، وعبر أي قناة.
2. **احموا البوابات لدى مزوّد المنبع.** تُمتصّ الهجمات الحجمية لدى المنبع أو لا تُمتصّ إطلاقاً. تعاقدوا على خدمة التخفيف للبوابات الموجهة إلى المواطنين وصفحات الدفع قبل وقوع أي حدث، واختبروها.
3. **راقبوا قوائم الأهداف.** نشرت Keymous Plus قوائم قبل ادعاءاتها وفيما بينها. تعاملوا مع أي قائمة جديدة تذكر قطاعكم بوصفها إشارة لرفع الجاهزية لمواجهة هجمات DDoS.

4. **توقّعوا أن يستغل الاحتيال الأخبار نفسها.** يُظهر تحذير وزارة الداخلية أن المحتالين يستغلون الأحداث نفسها. أرفقوا أي تنبيه بشأن DDoS بتنبيه بشأن الاحتيال والتصيّد الاحتيالي موجّه إلى الموظفين والعملاء.

الخلاصات الرئيسية

01

تركّزت ادعاءات نشطاء القرصنة بشأن هجمات DDoS ضد قطر في مارس 2026؛ ولم تؤكد أي جهة رسمية أو مؤسسة أن أياً منها تسبّب في انقطاع.

02

صنّفت NETSCOUT معظم الأهداف المقاسة على أنها مشغلو اتصالات سلكية؛ ولا تُظهر بياناتها ما إذا كانت المواقع التي ذكرتها المجموعات من بينها.

03

تروّج مجموعتان لخدمة الإغراق المأجورة نفسها؛ وفي الحالتين يبقى التخفيف لدى مزوّد المنبع هو الضابط الأساسي.

الفصل 7

الجهات الفاعلة في التهديد

يجيب هذا الفصل عن

من يقف وراء النشاط، وكيف ترتبط الجهات الفاعلة ببعضها، وماذا تقول التقارير العلنية عن كل منها؟

7

ملفات تعريف للجهات الفاعلة؛ جرى فحص التقارير العلنية لكل منها، وعُثر عليها لست منها

في هذا الفصل

7.1 كيف ترتبط الجهات الفاعلة

7.2 التجسس وبرامج التجسس التجارية (وفق إسناد المورّدين والباحثين)

7.3 الجهات الفاعلة في القرصنة الناشطة وهجمات DDoS

7.4 الفدية والابتزاز

7.5 شخصيات إجرامية رُصدت في Blackhole

7.6 النشرات التحذيرية من الوكالة الوطنية

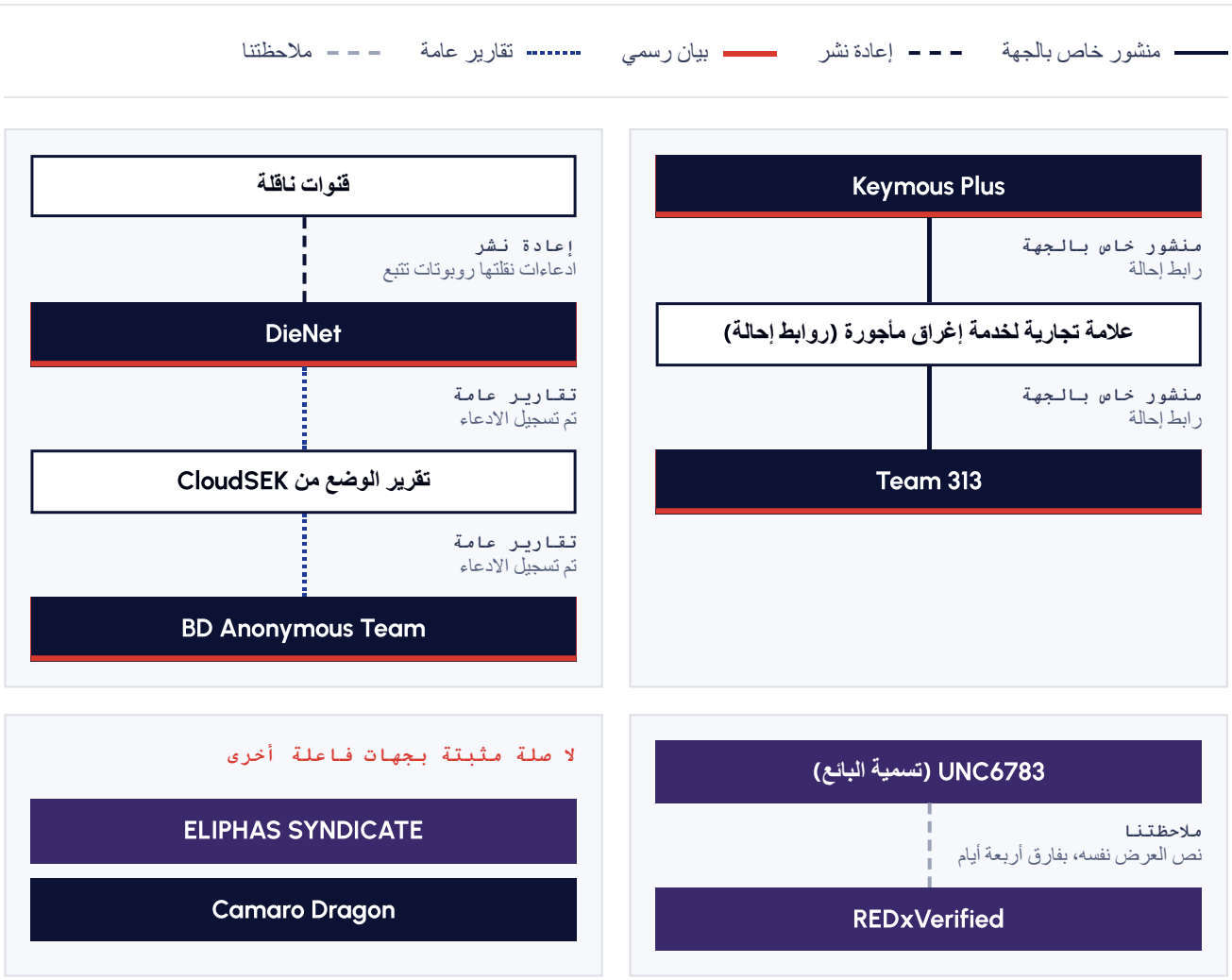
باختصار

أسندت Check Point حملة تجسس واحدة في 2026 إلى Camaro Dragon المرتبطة بالصين، وقيّمت حملة ثانية، بثقة منخفضة، بأنها متوافقة مع الصين. وأفاد Citizen Lab باستهداف 45 جهازًا على الأقل لدى Al Jazeera ببرنامج التجسس Candiru، وبإصابة أجهزة منها. وادّعى الهاكتفيست هجمات DDoS في مارس. ويحتفظ Ransompedia بإدراجات لثماني مؤسسات قطرية، معظمها شركات متوسطة الحجم. وذكر بائعو البيانات جهات في قطاعات الطاقة والمصارف والأمن. احظروا مرفقات الأرشيف والاختصارات الخارجية، وحدّثوا أنظمة الحافة التي تحذّر الوكالة من استغلالها، وتحققوا من كل ادعاء قبل التعليق عليه.

يفصل كل ملف تعريف بين **السلوك المرصود**، و**ادعاء الجهة الفاعلة نفسها**، و**ما يبقى دون حسم**، و**ما يعنيه ذلك للمؤسسات**. وتنطبق درجة الثقة على قضية محددة، لا على الجهة الفاعلة ككل.

7.1 كيف ترتبط الجهات الفاعلة

تربط الخريطة بين الجهات الفاعلة فقط حيث نملك أدلة، ويوضّح كل خط نوع الدليل: منشور الجهة الفاعلة نفسها، أو نقل من طرف ثالث، أو بيان رسمي، أو تقارير علنية. والخط يمثّل ارتباطاً، لا دليلاً على وجود مشغّل مشترك.



7.2 التجسس وبرامج التجسس التجارية (وفق إسناد المورّدين والباحثين)

Camaro Dragon

ربطتها Check Point بمجموعات وردت في التقارير باسم Mustang Panda وEarth Preta

تجسس (مرتبط بالصين وفق Check Point)

مرتبط بالصين (إسناد من المورّد؛ دون ذكر مستوى الثقة)

ضد أهداف قطرية، مارس 2026

1-2 مارس	نسخة من PlugX ضد أهداف قطرية في غضون يوم من التصعيد
مارس	طُعم: أرشيف يدّعي أنه صور لأضرار صواريخ، مع ملف اختصار

القطاعات المستهدفة

جهات حكومية وجهات مرتبطة بالطاقة (الملخص الأسبوعي لـ Check Point)

في التقارير العامة

- [S26] Check Point Research (9 مارس 2026): مفاتيح PlugX شوهدت في حملات سابقة منسوبة إلى Camaro Dragon
- [S27] التقرير الأسبوعي لـ Check Point (16 مارس 2026): ذكر أن الحملات استهدفت جهات حكومية وجهات مرتبطة بالطاقة

تقييمنا

أوضح نشاط تجسس موثّق ضد أهداف قطرية في 2026. تابعت الطُعوم الأخبار في غضون يوم؛ واعتمدت السلسلة على أن يفتح مستخدم أرشيفًا، لا على استغلال خادم.

درجة الثقة **إسناد من المورّد، دون ذكر مستوى الثقة**

أفادت Check Point بأن Camaro Dragon حاولت نشر متغيّر من PlugX ضد أهداف قطرية في غضون يوم واحد من التصعيد الإقليمي. وكان الطُّعم أرشيفاً متنكّراً في هيئة صور لأضرار صواريخ. وأطلق ملف اختصار سلسلةً انتهت باختطاف DLL لعميل تخزين سحابي مشروع. وربطت Check Point هذا النشاط بـ Camaro Dragon من خلال مفاتيح إعداد PlugX شوهدت في حملات سابقة تنسبها إلى تلك المجموعة [S26].

Unnamed China-aligned cluster

حملة محمّل Rust وCobalt Strike

تجسس (تقييم من المورّد بثقة منخفضة)

متوافق مع الصين، وفق تقييم Check Point بثقة منخفضة

ضد أهداف قطرية، مارس 2026

مارس	أرشيف محمي بكلمة مرور عن ضربات على منشآت النفط والغاز في الخليج، أُرسل على الأرجح بالبريد الإلكتروني
مارس	محمّل Rust، واختطاف DLL لمكوّن قارئ الشاشة، وCobalt Strike

القطاعات المستهدفة

مؤسسات قطرية (Check Point)؛ وجهات حكومية وأخرى مرتبطة بالطاقة وفق الملخص الأسبوعي للحملات

في التقارير العامة

- [S26] Check Point Research: قُيّمت بأنها متوافقة مع الصين بثقة منخفضة
- [S44] تصف Proofpoint مجموعة يُشتبه في توافقها مع الصين، تحمّل جانبيًا المكوّن نفسه من NVDA، وهو قارئ شاشة مفتوح المصدر، بطُعم يتناول النفط والغاز في الخليج، لتسليم Cobalt Strike إلى أهداف حكومية ودبلوماسية في الشرق الأوسط. ولا تصف أي مرحلة Rust ولا تسمّي قطر؛ ولا يربط أي من المورّدين بين الاثنتين

تقييمنا

محاولة تجسس ثانية منفصلة في الأسابيع نفسها. الإسناد ضعيف؛ والدروس الدفاعية هي نفسها كما في Camaro Dragon.

درجة الثقة **منخفضة (المورّد)**

استخدمت الحملة الثانية أرشيفاً محمياً بكلمة مرور يتناول ضربات على منشآت النفط والغاز في الخليج، يُرجّح أنه سُلّم عبر البريد الإلكتروني. واستغلّ محمّل مكتوب بلغة Rust لم يُرصد من قبل أحد مكوّنات قارئ الشاشة عبر اختطاف DLL، وسلّم Cobalt Strike [S26]. ووصفت Proofpoint بشكل منفصل مجموعة يُشتبه في توافقها مع الصين، حمّلت جانبيًا المكوّن نفسه من NVDA، وهو قارئ شاشة مفتوح المصدر، لتسليم Cobalt Strike [S44]. وحمل أرشيفها الموضوع نفسه المتعلق بالنفط والغاز في الخليج، واستهدفت جهات حكومية ودبلوماسية في الشرق الأوسط. ولا تصف Proofpoint أي مرحلة Rust ولا تسمّي قطر، ولا يربط أيٌّ من المزوّدَين بين الحالتين [S44]. ونُبقيهما منفصلتين.

تُعرض أدناه تقنيات مختارة من وصف Check Point. لم تنشر Check Point معرّفات ATT&CK؛ والمطابقة من إعدادنا.

التقنيات المذكورة في أبحاث الشركات الأمنية، بحسب التكتيك

الوصول الأولي	التنفيذ	التهرب الدفاعي	الاستمرارية / التهرب
T1566.001 تصيد موجّه بمرفق (أرشيف أُرسل على الأرجح بالبريد الإلكتروني؛ الحملة الثانية)	T1204.002 تنفيذ من المستخدم: ملف خبيث (ملف اختصار داخل الأرشيف)	T1036 التنكر (أرشيف يدّعي أنه صور)	T1574.001 اختطاف مسار التنفيذ: DLL (عميل التخزين السحابي ومكوّن قارئ الشاشة)

لم تنشر Check Point معرّفات ATT&CK. هذا التصنيف هو قراءة Odin لوصف Check Point الصادر في 9 مارس 2026، وقد رُوجع مقابل ATT&CK في 21 نوفمبر 2026؛ وهو ليس تصنيف المورّد. [S26]

برنامج تجسس تجاري ضد Al Jazeera. في 15 أكتوبر 2026 أفاد Citizen Lab بأن 45 جهازًا على الأقل لدى Al Jazeera استُهدفت في 2024 و2025، بهجمات لا تتطلب أي نقرة وصلت عبر إعلانات موجّهة على الإنترنت [S48]. ووجد أن أجهزة منها أُصيبت ببرنامج التجسس Candiru، وحلّل برمجية خبيثة استُخرجت من أحد تلك الأجهزة [S48]. ونشرت Al Jazeera النتائج في اليوم نفسه وأدانت هذا الاستهداف [S47]. ولا يذكر أي من التقريرين العميل الذي استُخدم البرنامج لصالحه [S47][S48].

دون حسم. بالنسبة إلى حملتي Check Point: الضحايا، وأي بيانات أُخذت، وما إذا نجحت أيٌّ من الحملتين. وذكر الملخص الأسبوعي لـ Check Point أن الحملات استهدفت جهات حكومية وأخرى مرتبطة بالطاقة [S27]. **المعنى.** تبعت الطُّعوم الأخبار في غضون يوم واحد. وبالنسبة للمؤسسات الحكومية ومؤسسات الطاقة، تتمثل الضوابط الحاسمة في حظر مرفقات الأرشيف والاختصارات الواردة من الخارج، والتنبيه عند قيام ملفات تنفيذية مشروعة وموقّعة بتحميل ملفات DLL من مجلدات المستخدمين، والبحث عن إشارات Cobalt Strike (beacons). ولم يظهر أي شيء من هاتين الحملتين في بيانات مواقع التسريب والمنتديات التي بحثنا فيها.

7.3 الجهات الفاعلة في القرصنة الناشطة وهجمات DDoS

Keymous Plus

Keymous

علامة ناشط قرصنة (هاكتفيست) لهجمات DDoS

لا يظهر انتماء معلن في المقتطفات المعروضة؛ وتدرجها CloudSEK ضمن الجهات الناشطة خلال التصعيد

في قطر، 2026

3 مارس	بوابة فوترة ودفع لخدمة عامة (B09)
12 مارس	13 موقعًا حكوميًا (B10)
24 مارس	خمس وزارات؛ وتقول إن بعض المواقع عادت للعمل (B15)
25 مارس	موقع في قطاع الطاقة ضمن 12 موقعًا إقليميًا للطاقة

الأهداف المُدّعاة

بوابات حكومية والوزارات وجهة تنظيمية مالية وبوابة فوترة ودفع لخدمة عامة وموقع في قطاع الطاقة

بكلماتهم

> *Some websites still down others are" up"* B15

في التقارير العامة

- [S29] CloudSEK (2 مارس 2026): أعلنت عن عمليات واسعة النطاق مزمعة ضد دول أخرى مع إثبات تقني محدود

تقييمنا

أكثر الجهات ادعاءً ضد قطر في بياناتنا. تحمل منشوراتها روابط إحالة إلى علامة تجارية لخدمة إغراق مأجورة (stresser)، ما يشير إلى قدرة مستأجرة؛ وتقرّ كلماتها نفسها بأن المواقع تعافت.

درجة الثقة **مرتفعة بأنها أطلقت الادعاءات؛ والأثر غير متحقق منه**

DieNet

DieNet Network V5

علامة ناشط قرصنة (هاكتفيست) لهجمات DDoS

موالية لإيران (وفق Unit 42)؛ أدرجتها CloudSEK ضمن الجهات الموالية لإيران

في قطر، 2026

28 فبراير-1 مارس	ادّعت هجمات DDoS على مواقع حكومية واتصالات ومطارات وبنوك في ست دول (CloudSEK)
6 مارس	تسعة منشورات نقل آلية تذكر مواقع حكومية قطرية (B12)

الأهداف المُدّعاة

مواقع حكومية

بكلماتهم

> *it may be down for you at the" moment"* B12

في التقارير العامة

- [S28] Unit 42: مجموعة ناشطي قرصنة موالية لإيران تنفذ هجمات DDoS في أنحاء الشرق الأوسط
- [S29] CloudSEK: الإسناد ذاتي، والتحقق التقني محدود
- [S34] DailyDarkWeb (6 مارس): ادّعت أن المواقع تعذّر الوصول إليها مؤقتًا؛ دون تأكيد

تقييمنا

جهة ادعاء إقليمية لهجمات DDoS تصلنا ادعاءاتها بشأن قطر عبر قنوات ناقلة آلية. تسجّل القنوات الناقلة فحوصًا انتهت مهلتها، لا انقطاعات.

درجة الثقة **متوسطة بأن DieNet أطلقت الادعاءات (منقولة)؛ والأثر غير متحقق منه**

Team 313

تطلق على نفسها اسم "المقاومة الإسلامية السيبرانية في العراق" (الاسم كما أوردته Unit 42)

ناشط قرصنة (هاكتفيست) (DDoS)

خلية ناشطي قرصنة موالية لإيران (وفق Unit 42)

في قطر، 2026

14 مارس	تدّعي تعطيل بوابة حكومية لمدة ساعة واحدة (B11)
15 مارس	تحديث: تدّعي توقفًا لعدة ساعات إضافية

الأهداف المُدّعاة

بوابة حكومية

بكلماتهم

> "completely disabling the website" B11

في التقارير العامة

- [S28] Unit 42: خلية نشطة من ناشطي القرصنة الموالين لإيران ادّعت هجمات على مواقع القوات المسلحة ووزارة الدفاع والمواقع الحكومية في الكويت

تقييمنا

جهة ادعاء إقليمية متكررة. ترتبط منشوراتها عن قطر بالعلامة نفسها لخدمة الإغراق المأجورة التي تستخدمها Keymous Plus؛ وهذه خدمة مشتركة، لا دليل على مشغّل مشترك.

درجة الثقة **مرتفعة بأنها أطلقت الادعاء؛ والأثر غير متحقق منه**

BD Anonymous Team

BD Anonymous

ناشط قرصنة (هاكتفيست) (DDoS)

قدّمت أفعالها في إطار مظالم جيوسياسية (وفق CloudSEK)

في قطر، 2026

28 فبراير-1 مارس	هجوم DDoS أُعلن ذاتيًا على خدمة إلكترونية لإحدى الوزارات (CloudSEK)
19 يونيو	تدّعي إسقاط موقع قوة أمنية ([B13])

الأهداف المُدّعاة

مواقع وزارية وأمنية

بكلماتهم

> "We have successfully took down" B13

في التقارير العامة

- CloudSEK [S29]: استهدفت خدمات إلكترونية لإحدى الوزارات بنشاط DDoS؛ والإسناد ذاتي

تقييمنا

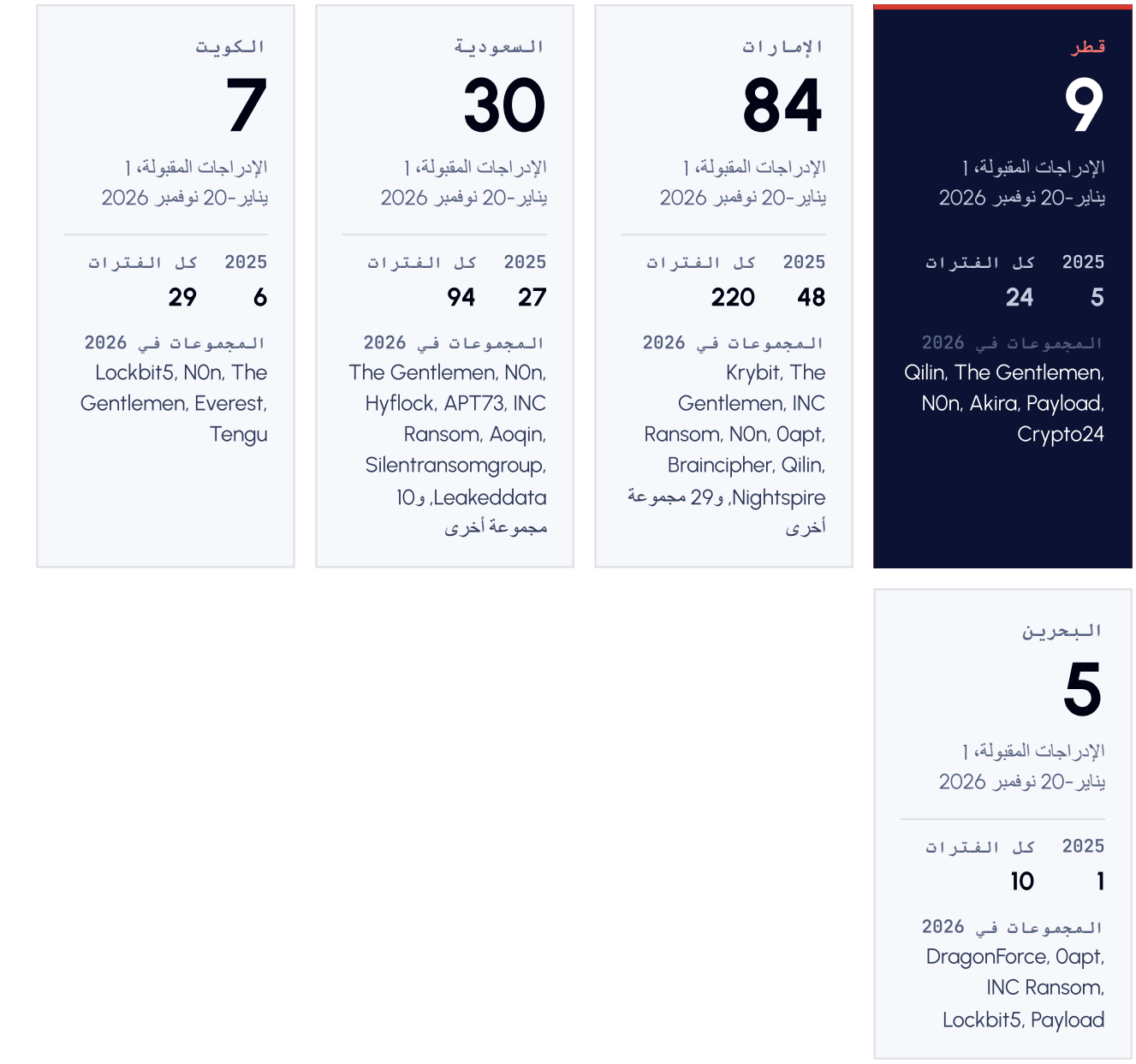
جهة ادعاء صغيرة لها واقعتان تخصان قطر. يذكر ادعاء يونيو دافعًا سياسيًا معلنًا؛ ونورده بوصفه دافع المجموعة نفسها.

درجة الثقة **متوسطة بأنها أطلقت الادعاءات؛ والأثر غير متحقق منه**

لا يُحتسب ضمن القرصنة الناشطة. نشرت عدة قنوات على Telegram ادعاءات بشأن أضرار مادية لحقت بمنشآت الطاقة القطرية خلال التصعيد. وهذه تعليقات على التصعيد، لا ادعاءات سيبرانية، ونستبعدها.

7.4 الفدية والابتزاز

تسعة إدراجات لدى مجموعات الفدية لجهات قطرية في 2026، مقابل 84 في الإمارات و 30 في السعودية وسبعة في الكويت وخمسة في البحرين



المصدر: الإدراجات المقبولة في Brandefense Ransompedia، جميع التواريخ، حتى 20 نوفمبر 2026 [S6]؛ وransomware.live للتحقق المتقاطع [S7].

يحتوي Ransompedia على تسعة إدراجات مقبولة لقطر مؤرخة بين 1 يناير و 20 نوفمبر 2026، تذكر ثماني مؤسسات متمايزة؛ وأُدرجت شركة مقاولات واحدة مرتين [S6]. نشرت Qilin ثلاثة من الإدراجات التسعة، وThe Gentlemen اثنين، وAkira وCrypto24 وN0n وPayload واحداً لكل منها. ويصنّف Ransompedia الإدراجات التسعة في القطاعات التالية: المقاولات (إدراجان)، والاستشارات، والاستشارات الهندسية، والاستشارات القانونية، والاتصالات، والتقنيات، والتصنيع، وإدراج واحد غير مصنّف.

ولا تطابق تصنيفاته دائمًا وصفنا للمؤسسة، كما في حالة المعهد البحثي المذكور أدناه. وفي الفترة نفسها يحتوي Ransompedia على 84 إدراجاً للإمارات، و 30 للسعودية، وسبعة للكويت، وخمسة للبحرين.

التحقق المتقاطع. يُدرج متتبّع علني سبع ضحايا قطريين في 2026 [S7]. وتقابل إدخالاته السبعة سبعة من إدراجات Ransompedia التسعة؛ ولا يتضمن الإدراجين الآخرين. ووسمت قنوات ناقلة أيضًا ادعاءين إضافيين بأنهما قطريان، أحدهما يذكر شركة صغيرة لا نكشف عنها؛ ولا يحتفظ بهما Ransompedia بوصفهما إدراجين قطريين، لذلك لا نحتسبهما. كما يُدرج المتتبّع تحت بلد آخر إدراجًا يخص شركة نضعها في قطر؛ وهي مؤسسة تاسعة (5§) نحتسبها خارج مؤسسات Ransompedia الثماني. وكررت القنوات الناقلة في مجموعة بياناتنا الادعاءات نفسها.

ماذا يعني ذلك. الإدراج هو ادعاء من مجموعة ابتزاز، لا اختراق مؤكد. وقد ذكرت ادعاءات الفدية ضد قطر في 2026 شركة بنية تحتية للاتصالات، ومعهداً بحثياً، ومكتب محاماة، وعدداً من المقاولين. والمقاولون والاستشاريون، من النوع الذي يخدم غالبًا قطاعي الطاقة والحكومة، جزء من نطاق الانكشاف. أما الحوادث غير المنشورة والحوادث التي جرى التفاوض بشأنها فلا تظهر هنا.

7.5 شخصيات إجرامية رُصدت في Blackhole

ELIPHAS SYNDICATE

ELIPHAS GANG

بائع بيانات | دافع مالي وفق روايتها

في قطر، 2026

10 مارس — تدّعي تفريغ قاعدة بيانات لشركة في قطاع الطاقة ومسح خادم (B02)

الأهداف المُدّعاة

شركة في قطاع الطاقة

بكلماتهم

> *WE DONT CARE ABOUT THE POLITICS WE CARE ABOUT THE PAYOUT" B02*

في التقارير العامة

تقييمنا

لم يُعثر على تقارير عامة موثوقة. جاء ادعاؤها بعد ثلاثة أسابيع من ادعاء ناشر آخر ضد الشركة نفسها (الحالة A).

درجة الثقة **مرتفعة بأنها أطلقت الادعاء؛ والادعاء غير متحقق منه**

شخصيات وعلامات أخرى، بالأسماء المستعارة فقط؛ دون جهات اتصال أو روابط أو هويات حقيقية.

الشخصية أو العلامة	الدور المرصود في 2026	ادعاؤها	دون حسم
Montaro (بحسب جهة رصد علنية)	ادعاء وصول في قطاع الطاقة (فبراير)	وصول إلى السحابة والهوية	ما إذا كانت هي من كتب منشور المنتدى (الحالة A)
ELIPHAS SYNDICATE	بائع على Telegram (مارس)	تفريغ قاعدة بيانات في قطاع الطاقة؛ ومسح الخادم	أي عيّنة؛ والصلة بـ Montaro
TheAshborn	بائع في منتدى اختراقات (مارس)	بيانات موظفي جهة أمنية	مصدر البيانات (الحالة B)
UNC6783 (اسم قناة أطلقه البائع على نفسه)	بائع في منتدى اختراقات (نوفمبر)	سجلات عملاء مصرف	أي تحقق (الحالة C)؛ والاسم وصف أطلقه البائع على نفسه
REDxVerified	بائع ثانٍ في منتدى للعرض نفسه الخاص بالمصرف (نوفمبر)	العرض نفسه، بالسعر نفسه	ما إذا كان البائع واحداً
X FORUMS (روبوت)	رافع آلي لملفات صغيرة، بما فيها نطاقات قطرية	لا يوجد	ليس شخصاً؛ بل روبوت توزيع
متاجر الأميال (عدة قنوات)	بائعو حسابات ولاء لشركات طيران، بما فيها حسابات ناقل خليجي	حسابات "مع إمكانية الوصول إلى البريد الإلكتروني"	أصحاب الحسابات؛ وما إذا كانت الحسابات مختطفة

7.6 النشرات التحذيرية من الوكالة الوطنية

تُعد خلاصة النشرات التحذيرية العلنية للوكالة الوطنية للأمن السيبراني (NCSA) أوضح إشارة رسمية إلى ما طُلب من المدافعين في قطر تحديثه. أحصينا 163 نشرة مؤرخة بين 11 يناير و 19 نوفمبر 2026 [S43]. وبحسب قراءتنا لعناوينها، يذكر 65 منها استغلالاً نشطاً أو ثغرة يوم الصفر، ويتعلق 49 منها بمنتجات الشبكات أو الوصول عن بُعد أو الأمن من مزوّدين مثل Cisco وFortinet وCitrix وIvanti

وPalo Alto Networks وSonicWall. وفي مارس حذّرت الوكالة أيضاً مستخدمي iPhone من ثغرات في iOS تُستغل بشكل نشط، وذكرت أن الإصدارين iOS 13 و 14 مستهدفان على وجه التحديد [S38].

الخلاصات الرئيسية

01

أسندت Check Point حملة تجسس واحدة في 2026 ضد أهداف قطرية إلى Camaro Dragon، وقيّمت حملة ثانية بأنها متوافقة مع الصين بثقة منخفضة.

02

تروّج مجموعتان من نشطاء القرصنة لخدمة الإغراق المأجورة نفسها؛ والخدمة المشتركة ليست مشغّلاً مشتركاً.

03

ذكرت ادعاءات الفدية مقاولين وموردي بنية تحتية أكثر مما ذكرت أسماء كبرى معروفة.

الفصل 8

اقتصاد الاحتيال

يجيب هذا الفصل عن

كيف يحوّل المجرمون الهويات والحسابات والبطاقات القطرية إلى أموال، ومن أي شيء حذّرت السلطات؟

32 USD

السعر المطلوب الوسيط لحساب مصرفي أو حساب محفظة في المنشورات المنقّاة

في هذا الفصل

8.1 الحسابات المصرفية وحسابات المحافظ والمنصات

8.2 بيانات البطاقات في المنشورات: رؤية محدودة

8.3 حسابات الولاء والبريد الإلكتروني

8.4 روابط الدفع وعمليات الاحتيال باسم العلامات التجارية

8.5 خدمات الهوية وKYC والاتصالات الهاتفية

8.6 الأسعار في سياقها

8.7 من أي شيء حذّرت السلطات

باختصار

تظهر قطر في السوق السرية أساساً بوصفها سوقاً. يُدرج البائعون بطاقات قطرية، وحسابات تداول وبريد إلكتروني مسجّلة في قطر، وحسابات ولاء لشركات طيران، إلى جانب عشرات الدول الأخرى. وحذّرت السلطات مراراً من رسائل تنتحل صفة جهات حكومية والهيئة العامة للضرائب وشركات معروفة. أكّدوا تعليمات الدفع عبر قناة مستقلة، واحموا حسابات الولاء والبريد الإلكتروني بمصادقة MFA قوية، وافترضوا أن الانتحال سيلي كل حدث إخباري كبير.

8.1 الحسابات المصرفية وحسابات المحافظ والمنصات

يُعد الاتجار بالحسابات عائلة كبيرة من المنشورات المنقّاة (1,635–1,756 منشوراً)، لكنه يحتاج إلى قراءة متأنية. إذ يتعلق كثير من منشورات تأجير الحسابات بمصرف تركي لا بمصرف قطري. أما المنشورات الخاصة بقطر فمختلفة. فالمشترون يطلبون حسابات "جاهزة" على منصات تداول أجنبية مسجّلة بهويات قطرية، عادةً مقابل 25–40 USD للحساب الواحد. وتتيح هذه الحسابات للمشتري تحريك الأموال تحت هوية شخص آخر جرى التحقق منها. وتُظهر المنشورات وجود طلب وعروض؛ لكنها لا تُظهر أن أي حساب فُتح لدى مؤسسة قطرية.

8.2 بيانات البطاقات في المنشورات: رؤية محدودة

> **نطاق أرقام البطاقات**
>
> تغطي أرقام البطاقات في هذا التقرير فقط بطاقات الدفع التي ظهرت بنص واضح داخل منشورات الويب المظلم التي جمعناها لهذا التقرير. وتكتشف Brandefense البطاقات المسروقة بطرق أخرى عديدة لا يغطيها هذا التقرير. وهذه الأرقام ليست مقياساً لسرقة البطاقات أو لخسائر الاحتيال في قطر.

ضمن هذا النطاق المحدود، ظهرت 110 بطاقات متمايزة مرتبطة بقطر بنص واضح في المنشورات المجمّعة. من بينها 85 بطاقة نُسبت إلى أحد سبعة مصارف قطرية مسمّاة، أما الـ 25 الأخرى فوُصفت بأنها قطرية فقط، دون جهة إصدار. وظهرت 81 من الـ 110 في مخرجات أدوات فحص البطاقات. ولا ينشر هذا التقرير أي بيانات بطاقات (الملحق A.6) [S8]. والإشارة المفيدة لجهات الإصدار هي نمط الفحص نفسه: دفعات من البطاقات تُختبر بتفويضات صغيرة عبر بوابات التجار (الفصل 9).

8.3 حسابات الولاء والبريد الإلكتروني

عرضت "متاجر الأميال" على Telegram للبيع حسابات ولاء لشركات طيران وفنادق في 2026، مع ذكر أرصدة النقاط و"الوصول الكامل إلى البريد الإلكتروني". وظهر برنامج ناقل خليجي في عشرات من هذه المنشورات إلى جانب شركات طيران أخرى [S1]. والأهم هو عرض الوصول إلى البريد الإلكتروني. فإن صحّ، فهو يشير إلى أن البائع يسيطر على صندوق البريد المستخدم لإعادة تعيين الحساب، وهو ما يتسق مع بيانات اعتماد مسروقة أو سجلات برامج سرقة المعلومات، لا مع اختراق لشركة الطيران. وتُحوّل نقاط الولاء إلى تذاكر وقسائم يصعب استردادها.

بطاقة الدليل B14 | 1 يناير 2026

Miles shop قناة متجر لحسابات الولاء · Telegram · الإنجليزية

النص الأصلي

```
[Gulf carrier] 310k point available
with email access. Escrow
```

الترجمة

[ناقل جوي خليجي] 310k نقطة متاحة مع الوصول إلى البريد الإلكتروني. ضمان (Escrow)

ما يمكن إثباته	عرض لحساب ولاء برصيد نقاط ووصول إلى صندوق البريد المرتبط به؛ وتتكرر عروض مشابهة على مدار العام.
ما لم يثبت	صاحب الحساب، أو كيفية الحصول عليه.

8.4 روابط الدفع وعمليات الاحتيال باسم العلامات التجارية

يسيء مستخدمو البطاقات المسروقة أيضًا استخدام صفحات دفع قطرية مشروعة. ففي مارس شاركت قناة صفحة عامة لدفع الفواتير بوصفها وسيلة لإنفاق بطاقات مسروقة. وفي سبتمبر وأكتوبر عرض بائعون روابط فواتير من بوابة دفع قطرية على "المحمّلين" مقابل 65–70% من قيمتها الاسمية [S1]. وعرض بائعون في مايو ويونيو صفحات احتيال مصممة على غرار مصرف قطري كبير، وفي أبريل استخدمت منصة استثمار مزيفة اسم المصرف نفسه. الصفحات والروابط خدمات حقيقية؛ والإساءة تكمن في هوية من يدفع وبأي بطاقة.

8.5 خدمات الهوية وKYC والاتصالات الهاتفية

تعرض منشورات KYC والمستندات (534–567 منشوراً منقّى) خدمات تحقق، وقوالب مستندات، وحسابات جرى التحقق منها بهويات قطرية. ويُدرج بائعو خدمات الاتصالات الهاتفية قطر ضمن الوجهات لإرسال الرسائل النصية، وانتحال هوية المتصل، وروبوتات كلمات المرور لمرة واحدة. وبالاقتران مع مجموعات بيانات الهوية الواردة في §4.4، تخفّض هذه الخدمات كلفة انتحال صفة المقيمين والمؤسسات.

8.6 الأسعار في سياقها

المنتج (المنشورات المنقّاة)	السعر المطلوب الوسيط	النطاق
بطاقة (للبطاقة الواحدة)	USD 14	USD 10–25

المنتج (المنشورات المنقّاة)	السعر المطلوب الوسيط	النطاق
عرض بيانات أو عملاء محتملين	USD 15	USD 10-30
قائمة دمج (combolist)	USD 27	USD 15-35
حساب مصرفي أو محفظة أو منصة	USD 32	USD 25-60
خدمة KYC أو مستندات	USD 50	USD 20-100
عرض وصول	USD 171	واسع، وقيم قليلة

الأسعار هي أسعار مطلوبة من أقلية من المنشورات التي تذكر سعراً؛ وهي لا تقيس القيمة السوقية ولا المبيعات المكتملة. والنطاق هو النصف الأوسط من الأسعار المذكورة (من المئين 25 إلى المئين 75)، ولذلك فهو ليس المدى الكامل. وتقع العروض المنفردة خارجه، مثل ملف الجهة الأمنية بسعر USD 10,000 وملف المصرف بسعر USD 1,500 في الفصل 4.

8.7 من أي شيء حذّرت السلطات

تُظهر المنشورات العروض. أما التحذيرات أدناه فتصف ما رأته السلطات القطرية وأبلغت به الجمهور؛ وقد نُشرت جميعها في 2026.

التاريخ	الجهة	مضمون التحذير
3 فبراير	الوكالة الوطنية للأمن السيبراني	قرار ملزم (رقم 3 لسنة 2025) بحق شركة في القطاع الرياضي بعد خرق للبيانات الشخصية، بسبب عدم كفاية تدابير الحماية [S25]
26 فبراير	الهيئة العامة للضرائب	رسائل بريد إلكتروني ورسائل نصية تصيّدية منسّقة تنتحل صفة الهيئة، بطُعوم تتعلق باسترداد مبالغ وتحديث البيانات والتحقق من الحساب [S36]
22 مارس	الوكالة الوطنية للأمن السيبراني	ثغرات في iOS تُستغل بشكل نشط؛ الأجهزة الأقدم بإصداري iOS 13 و 14 مستهدفة على وجه التحديد؛ يجب التحديث فوراً [S38]
24 مارس	وزارة الداخلية	اتصالات ورسائل تنتحل صفة جهات حكومية للحصول على البيانات المصرفية والتحويلات ورموز التحقق لمرة واحدة [S35]
19 سبتمبر	الوكالة الوطنية للأمن السيبراني	رسائل نصية ورسائل بريد إلكتروني احتيالية تنتحل صفة جهات حكومية وشركات كبرى [S45]

التاريخ	الجهة	مضمون التحذير
28 سبتمبر	وزارة الداخلية	مواقع إلكترونية مزيفة تنسخ ألوان شركات معروفة وخطوطها وتصاميمها؛ والابتزاز الإلكتروني يُعاقب عليه بالسجن مدة تصل إلى ثلاث سنوات [S37]
3 نوفمبر	هيئة تنظيم الاتصالات	سياسات جديدة لسجل نطاقات .qa اعتباراً من 22 أكتوبر للحد من إساءة استخدام النطاقات والانتحال والتصيّد الاحتيالي [S39]

ما يعنيه ذلك للمدافعين. تصف التحذيرات الرسمية وعروض السوق السرية نقطة الضعف نفسها: الثقة في اسم مألوف. إذ تُقلِّد الجهات الحكومية والهيئة العامة للضرائب والعلامات التجارية الكبرى عبر الرسائل النصية والبريد الإلكتروني والاتصالات والمواقع الإلكترونية المشابهة. وفي أبريل 2025 أدرجت Silent Push قطر ضمن الدول المستهدفة من عملية التصيّد بالرسائل النصية التي تتخذ من الصين مقراً لها والتي تسمّيها [S46] Smishing Triad. والضوابط إجرائية وتقنية: التأكيد المستقل لتعليمات الدفع عبر قناة أخرى، ومصادقة MFA مقاومة للتصيّد، ومراقبة العلامات التجارية والنطاقات، وتحذيرات عامة تسمّي القنوات الحقيقية.

الخلاصات الرئيسية

01

تظهر قطر في الغالب سوقاً في المنشورات التي جمعناها: تُباع البطاقات والحسابات التي جرى التحقق منها وحسابات الولاء إلى جانب دول كثيرة أخرى.

02

تغطي أرقام البطاقات فقط البطاقات التي شوهدت بنص واضح في المنشورات المجمّعة (§8.2).

03

انتحال صفة الجهات الحكومية والعلامات التجارية الكبرى هو نمط الاحتيال الذي حذّرت منه السلطات أكثر من غيره.

الفصل 9

تحليل معمّق للقطاع المصرفي والمالي

يجيب هذا الفصل عن

أين يقع الانكشاف المرئي للمصارف القطرية: في المصرف نفسه، أم لدى موظفيه، أم لدى عملائه؟

9 of 9

المصارف المُصدِرة للبطاقات في قائمتنا التي لديها إدراج حالي لبيانات اعتماد، وهو أول بند يجب فرزه

باختصار

كان لدى كل مصرف من المصارف التسعة المُصدِرة للبطاقات في قائمتنا بيانات اعتماد مرتبطة بنطاقه مدرجة للبيع في يوم الفحص. ويقع معظم الانكشاف المرئي الآخر على الأرجح في جانب العملاء: 4,415 ارتباطاً بأجهزة غير مصنّفة كأجهزة موظفين ونشاط أدوات فحص البطاقات. أما الإشارة في جانب الموظفين فصغيرة: 64 جهازاً مصنّفاً كجهاز موظف في ستة مصارف. افرزوا كل إدراج حالي لبيانات الاعتماد أولاً، ثم تحققوا من أجهزة الموظفين، وراقبوا حالات الرفض الناتجة عن أدوات الفحص على نطاقات BIN الخاصة بكم.

يغطي هذا الفصل المصارف التسعة المُصدِرة للبطاقات من بين 30 مؤسسة مصرفية ومالية في الفصل 3؛ أما الـ 21 الأخرى فهي المصرف المركزي، والبنية التحتية للسوق، ودور الصرافة، وشركات الاستثمار، ومزوّدو خدمات الدفع. ولهذا يختلف رقم 4,415 جهازاً غير مصنّف كجهاز موظف هنا عن رقم 5,257 للقطاع بأكمله، ولهذا تكون 9 من مؤسسات القطاع الـ 12 التي لديها إدراج حالي جهاتِ إصدار. البيانات مجمّعة فقط؛ ولا تُذكر أسماء المصارف منفردة.

9 of 9

مصارف مُصدِرة للبطاقات لديها إدراج حالي لبيانات اعتماد (9 من مؤسسات القطاع الـ 12 التي لديها إدراج حالي)

9 of 9

جهات إصدار لديها ارتباطات بأجهزة غير مصنّفة كأجهزة موظفين (4,415 إجمالاً؛ الملكية والإصابة الحالية غير متحقق منهما)

6 of 9

جهات إصدار لديها أجهزة مصنّفة كأجهزة موظفين (64 إجمالاً)

8 of 9

مصارف مُصدِرة للبطاقات تطبّق DMARC (16 من 30 على مستوى القطاع)

7 of 9

مصارف مُصدِرة للبطاقات ظهرت بطاقاتها بنص واضح في المنشورات المجمّعة (85 من البطاقات الـ 110 تذكر أحدها؛ نطاق محدود، §8.2)

تستحوذ جهات الإصدار الثلاث الأولى على 71% من البطاقات المنسوبة و 85% من الارتباطات بأجهزة غير مصنّفة كأجهزة موظفين.

ماذا يعني ذلك للمصارف.

1. **الإدراجات الحالية أولاً.** كان لدى جهات الإصدار التسع جميعها إدراج حالي في يوم الفحص؛ طبّقوا القرار 1 (البتّ خلال 5 أيام عمل).
2. **انكشاف الموظفين صغير لكنه حقيقي.** تمثّل الأجهزة الـ 64 المصنّفة كأجهزة موظفين في ستة مصارف المجموعة الفرعية ذات الصلة بالاختراق. وبعد الإدراجات الحالية، تستحق هذه الأجهزة أولوية في التحقق على المجموع الأكبر بكثير للأجهزة غير المصنّفة كأجهزة موظفين.
3. **الارتباطات بأجهزة غير مصنّفة كأجهزة موظفين هي الانكشاف الأكبر.** هناك 4,415 ارتباطاً بأجهزة غير مصنّفة كأجهزة موظفين، والأرجح أن معظمها أجهزة عملاء. والملكية، والإصابة الحالية، وما إذا كانت أي جلسة أو كلمة مرور مخزّنة لا تزال صالحة، كلها أمور غير متحقق منها. وينبغي لفرق مكافحة الاحتيال استخدام إشارات مخاطر الجهاز والجلسة عند تسجيل الدخول وعند تغيير المستفيدين، لا الاكتفاء بالتحقق من كلمة المرور.
4. **فحص البطاقات مؤشر سابق يمكن اكتشافه.** تختبر روبوتات الفحص البطاقات بتفويضات صغيرة عبر بوابات التجار. ويمكن لجهات الإصدار اكتشاف تجمّعات المحاولات المرفوضة منخفضة القيمة الواردة من بوابات أجنبية على نطاقات BIN الخاصة بها، وفحص إشارات التفويض والاحتيال للبطاقات المعنية، وإعادة إصدار البطاقات التي يتأكد تعرّضها للخطر وفق سياسة جهة الإصدار.
5. **ادعاء البيانات المتكرر يحتاج إلى رد مُعدّ مسبقاً.** ذُكر مصرف كبير واحد في عروض بيانات في أبريل وأغسطس ونوفمبر (الحالة C). وينبغي للمصارف أن تكون قادرة على مقارنة البنية المدّعاة للبيانات مع صادراتها الخاصة خلال يوم واحد، وعلى إحاطة العملاء إذا تأكدت صحة عيّنة.

أعمال تعزيز مرونة القطاع جارية. أجرى مصرف قطر المركزي أول تمرين للمرونة السيبرانية على مستوى القطاع، وفقاً للتغطية الإعلامية لمراجعة الاستقرار المالي لعام 2025 [S41]. كما تعمل المصارف بموجب لائحته للحوسبة السحابية الصادرة في أبريل 2024 [S23].

الخلاصات الرئيسية

01

تأتي الإدراجات الحالية لبيانات الاعتماد لدى جهات إصدار البطاقات التسع جميعها أولاً، ثم الأجهزة الـ 64 المصنّفة كأجهزة موظفين؛ كما تحتاج الأجهزة الـ 4,415 غير المصنّفة كأجهزة موظفين إلى التحقق أيضاً.

02

تطبّق جهات إصدار البطاقات DMARC على نطاق واسع (8 من 9)؛ بينما لا تطبّقه في الغالب مؤسسات القطاع المالي الأخرى (8 من 21).

03

حالات الرفض الناتجة عن أدوات فحص البطاقات على نطاقات BIN الخاصة بكم مؤشر سابق يمكن اكتشافه.

الفصل 10

الاستجابة التنظيمية والوطنية

يجيب هذا الفصل عن

ما القواعد القطرية التي تحدد مهل الإبلاغ عن الحوادث السيبرانية، وما الذي ينبغي أن يكون لدى المؤسسة قبل الحادثة التالية؟

72 h

للإخطار باختراق جسيم للبيانات الشخصية بموجب إرشادات الخصوصية الصادرة عن الوكالة

في هذا الفصل

10.1 ما تمكّنا من التحقق منه

10.2 نظام الخصوصية مُطبَّق فعليًا

10.3 أي المهل تنطبق عليك

باختصار

تقع القواعد السيبرانية في قطر أساسًا ضمن اختصاص الوكالة الوطنية للأمن السيبراني (NCSA): استراتيجية وطنية، ومعيار أساسي، ومنذ أكتوبر 2026 أطر وطنية ومؤسسية لإدارة المخاطر. وقد تسري عدة مهل في آن واحد بعد حادثة واحدة. ومنها 72 ساعة لاختراق جسيم للبيانات الشخصية بموجب إرشادات الوكالة، وواجبات إبلاغ بموجب المعيار الوطني وأطر 2026 لم يتمكن هذا الإصدار من تأكيد مهلها. حدّد المهل التي تنطبق عليك، واطلب المهل غير المؤكدة كتابيًا من الوكالة، وسمِّ من يبدأ كلًا منها.

10.1 ما تمكّنا من التحقق منه

يسرد الجدول الأدوات التنظيمية التي راجعناها، مع أهم الواجبات أثناء الحادثة. ويشير عمود التنبيه إلى ما لم يتمكن هذا الإصدار من تأكيده.

الإجراء	ما تمكّنا من التحقق منه	الوضع والتحفظ
الوكالة الوطنية للأمن السيبراني	أُنشئت بموجب قرار أميري رقم (1) لسنة 2021 بإنشاء الوكالة الوطنية للأمن السيبراني، المؤرخ في 14 مارس 2021 والمنشور في 24 مارس 2021. وتشمل اختصاصاتها المدرجة الاستراتيجية الوطنية، والمعايير والامتثال، وتصنيف مؤسسات القطاعات الحيوية، والخطة الوطنية للاستجابة للحوادث، وترخيص مزودي خدمات الأمن السيبراني، وتنفيذ قانون حماية خصوصية البيانات الشخصية [S14]	يجب على الجهات الحكومية التعاون مع الوكالة، وتظل مسؤولة عن حماية أنظمتها [S14]

الإجراء	ما تمكّنا من التحقق منه	الوضع والتحفظ
الاستراتيجية الوطنية للأمن السيبراني 2024-2030	خمس ركائز، من مرونة البنية التحتية الوطنية الحيوية إلى التعاون الدولي، يتابعها مكتب للاستراتيجية داخل الوكالة [S15]	استراتيجية وليست واجبًا في حد ذاتها؛ تتبع الواجبات من المعايير أدناه
المعيار الوطني لضمان أمن المعلومات (الإصدار V2.1، مايو 2023)	وفق قراءتنا، ينص المعيار على أن الضوابط الأساسية "إلزامية ويجب تطبيقها". ويحدد الضابط IM 8 مهلة للإبلاغ عن الحوادث الحرجة إلى الوكالة [S16]	لم تُؤكَّد مهلة IM 8 في هذا الإصدار؛ اطلبها كتابيًا من الوكالة. ويجب أولًا تصنيف الأصول وفق السياسة الوطنية لتصنيف البيانات [S16]
الإطاران الوطني والمؤسسي لإدارة مخاطر أمن المعلومات (الإصدار V1.0)	أُطلقا في 5 أكتوبر 2026 [S18]. ووفق قراءتنا لنص الإطارين، يُعدّ اعتمادهما "مستحسنًا بشدة"، ويتضمن الإطاران إبلاغ الوكالة عن المخاطر وتقديم إقرار سنوي [S17]	لم تُؤكَّد واجبات الإبلاغ ولا توقيتها في هذا الإصدار؛ اطلب توضيحًا مكتوبًا من الوكالة. ولا يوضح النص ما إذا كان واجب الإبلاغ يسري على جهات غير تلك التي تعتمد الإطارين. جديد في 2026؛ يُتوقع صدور إرشادات لاحقة بشأن النطاق والصيغة
ضوابط المشاركين في الأسواق المالية (الإصدار V1.0، مارس 2026)	ضوابط مكملة للمعيار الوطني للجهات الخاضعة لتنظيم هيئة قطر للأسواق المالية، أُعلن عنها مع برنامج للامتثال [S17][S18]	تنطبق على المشاركين في السوق، لا على كل شركة مالية؛ أكّد الإصدار مع الوكالة
قانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية	يُعاقب على الدخول غير المشروع بالحبس مدة تصل إلى ثلاث سنوات وغرامة تصل إلى 500,000 ريال قطري؛ وعلى التهديد والابتزاز عبر الإنترنت بالحبس مدة تصل إلى ثلاث سنوات وغرامة تصل إلى 100,000 ريال قطري؛ ويجوز تغريم الشخص المعنوي بما يصل إلى 1,000,000 ريال قطري. ويجب على الجهات الحكومية وشركاتها الإبلاغ عن الجرائم "فور اكتشافها" والاحتفاظ ببيانات تقنية المعلومات مدة لا تقل عن 120 يومًا، ويحتفظ مزودو الخدمات بمعلومات المشتركين مدة سنة واحدة [S19]	أضاف القانون رقم (11) لسنة 2025 جريمة نشر صور الأشخاص في الأماكن العامة دون موافقتهم [S20]
قانون رقم (13) لسنة 2016 بشأن حماية خصوصية البيانات الشخصية	يجب على المتحكم إخطار الفرد والإدارة المختصة بأي اختراق قد يسبب ضررًا جسيمًا. وتصل الغرامات إلى 1,000,000 ريال قطري أو 5,000,000 ريال قطري بحسب المادة المخالَفة [S21]	لا يحدد القانون مهلة بالساعات؛ وتحدد إرشادات الوكالة 72 ساعة للاختراقات الجسيمة [S22]. وتعمل الوكالة بصفتها الجهة المختصة [S21]

الإجراء	ما تمكّنا من التحقق منه	الوضع والتحفظ
لائحة الحوسبة السحابية الصادرة عن مصرف قطر المركزي	صدرت في أبريل 2024 للجهات المرخصة من مصرف قطر المركزي، لتنظيم استخدامها للخدمات السحابية [S23]	لم تُؤكَّد في هذا الإصدار التزاماتها بشأن موقع البيانات والموافقة المسبقة؛ تحقّق منها، ومن قواعد المصرف ذات الصلة بالتعامل مع البيانات، لدى مصرف قطر المركزي. تُقرأ مع تعليمات مصرف قطر المركزي للبنوك بشأن الإبلاغ عن الحوادث، والتي لم نتمكن من قراءة ملحق المهل الزمنية فيها
لوائح حماية البيانات لمركز قطر للمال 2021	بموجب المادة 31، يجب على المتحكم في البيانات إخطار مكتب حماية البيانات في مركز قطر للمال بأي اختراق للبيانات الشخصية خلال 72 ساعة. ويُستثنى ذلك إذا قرر المتحكم أن الاختراق لا يُرجَّح أن يشكّل خطرًا على حقوق أصحاب البيانات ومصالحهم المشروعة [S24]	يقع هذا الواجب على المتحكم؛ ولا يتناول الجدول واجبات المعالجين أو الأطراف الأخرى. نظام مستقل عن قانون الخصوصية الوطني
سياسات سجل نطاقات qa.	دخلت السياسات المحدّثة حيز التنفيذ في 22 أكتوبر 2026، مع قواعد أوضح للأهلية تهدف إلى الحد من إساءة استخدام النطاقات وانتحال الهوية والتصيد الاحتيالي [S39]	لا تشمل النطاقات المشابهة تحت نطاقات المستوى الأعلى الأخرى

10.2 نظام الخصوصية مُطبَّق فعليًا

في فبراير 2026 أعلن مكتب الخصوصية التابع للوكالة الوطنية للأمن السيبراني عن قرار ملزم (رقم 3 لسنة 2025) بحق شركة في القطاع الرياضي إثر اختراق للبيانات الشخصية. وخلص إلى قصور تدابير الحماية التقنية والإدارية والمادية بموجب المواد 8(3) و 13 و 14 من قانون الخصوصية، وأمر الشركة بمراجعتها وتعزيزها [S25]. ولم يُكشف عن اسم الشركة. وبحسب التقرير، رصدت فرقُ الوكالة المتخصصة الاختراقَ بنفسها [S25]. والدرس للمؤسسات أن جهة تنظيم الخصوصية تتحرك بشأن الاختراقات التي ترصدها بنفسها، لا بناءً على الشكاوى فحسب.

10.3 أي المهل تنطبق عليك

قد تبدأ عدة مهل للإبلاغ من حدث واحد. يطبّق الجدول الأدوات المذكورة أعلاه على أربع حالات شائعة. وهو أداة تخطيط، لا استشارة قانونية.

المؤسسة	المهل الواجب التخطيط لها	الإجراء الآن
جهة حكومية أو شركة مملوكة للدولة	حادثة حرجة إلى الوكالة ضمن مهلة المعيار الوطني (اطلبها كتابيًا من الوكالة) [S16]؛ إبلاغ فوري عن جريمة إلكترونية [S19]؛ إبلاغ المخاطر بموجب أطر 2026 (النطاق والتوقيت غير مؤكدين؛ اطلب توضيحًا من الوكالة) [S17]؛ اختراق جسيم للبيانات الشخصية خلال 72 ساعة [S22]	سمِّ مسؤولًا واحدًا عن الإبلاغ عن الحوادث للمهل الأربع، مع نائب له
بنك أو مزود خدمات دفع مرخص من مصرف قطر المركزي	الإبلاغ عن الحوادث إلى مصرف قطر المركزي (المهلة غير متحقق منها)؛ اختراق الخصوصية خلال 72 ساعة إذا كان جسيمًا [S22]؛ قواعد مصرف قطر المركزي للسحابة والبيانات (التزامات يجب تأكيدها مع المصرف) [S23]	ارسم مساري مصرف قطر المركزي والوكالة في دليل إجراءات واحد
شركة في مركز قطر للمال	بصفتك متحكمًا، مكتب حماية البيانات في مركز قطر للمال خلال 72 ساعة، ما لم يُرجَّح أن الاختراق لا يشكّل خطرًا على حقوق أصحاب البيانات [S24]	وثّق تقييم المخاطر وراء أي قرار بعدم الإخطار؛ وتأكد من نظام الخصوصية الذي يغطي كل مجموعة بيانات
أي مؤسسة أخرى تحتفظ ببيانات شخصية	اختراق جسيم للبيانات الشخصية خلال 72 ساعة [S22]؛ معيار الوكالة حيثما ينطبق عليك [S16]	احتفظ بسجل للاختراقات ومسودة إخطار معبأة مسبقًا

ما ينبغي أن يفعله مسؤولو أمن المعلومات الآن. أكّد كتابيًا الأدوات التي تنطبق على مؤسستك وعلى الجهة التنظيمية لقطاعك. سمِّ الشخص الذي يُبلغ الوكالة الوطنية للأمن السيبراني وجهة تنظيم الخصوصية، وبالنسبة للشركات المالية مصرف قطر المركزي أو مكتب مركز قطر للمال. تدرّب على مهلة الحادثة الحرجة، لأن تصنيف الحادثة كحرجة والإبلاغ عنها ضمن المهلة يتطلبان مسار قرار قائمًا مسبقًا. احتفظ بسجلات مؤرخة للضوابط، لأن أطر 2026 ستتبعها إرشادات إضافية.

الخلاصات الرئيسية

01

خطّط لعدة مهل: 72 ساعة لاختراق جسيم للبيانات الشخصية، ومهلة الحوادث الحرجة، وواجبات أطر المخاطر لعام 2026؛ اطلب مهل الأخيرتين كتابيًا من الوكالة.

02

أعلنت جهة تنظيم الخصوصية في فبراير 2026 قرارًا ملزمًا (رقم 3 لسنة 2025) إثر اختراق رصدته فرقها.

03

تخضع البنوك إضافةً إلى ذلك لقواعد مصرف قطر المركزي، بما فيها لائحة الحوسبة السحابية لعام 2024؛ أكّد التزامات موقع البيانات مع المصرف.

الفصل 11

التوقعات

يجيب هذا الفصل عن

ما الذي ينبغي أن تخطط له المؤسسات القطرية لاحقًا، وما الأدلة التي قد تغيّر هذه الخطة؟

5

أحكام رئيسية، لكل منها مؤشر للمتابعة

في هذا الفصل

11.1 الأحكام الرئيسية | 11.2 ما الذي قد يغيّر التقييم | 11.3 سيناريوهات مشروطة

باختصار

خطّط لأنواع الأدلة ذاتها، لا لتهديد جديد: انكشاف الهوية الذي يبقى غير مرئي حتى يُستخدم، وهجمات DDoS التي يشنها نشطاء القرصنة بدافع الأخبار. ويضاف إليها طُعوم التجسس في المرفقات، وادعاءات البيانات المتكررة ضد كبار أصحاب العمل. لا تتوفر لدينا سلسلة زمنية قابلة للمقارنة للقول إن أيًا منها في تزايد. غيّر الخطة عندما تتغير الأدلة أدناه، لا وفق التقويم.

11.1 الأحكام الرئيسية

الحكم	درجة الثقة	الأساس والحدود
انكشاف الهوية (الأجهزة، وسجلات برامج سرقة المعلومات، وإدراجات بيانات الاعتماد للبيع) هو أوسع المخاطر القابلة للقياس انتشارًا لدى المؤسسات الرائدة في قطر	عالية بالنسبة لقائمة المؤسسات الـ 250	182 لديها أجهزة، و 213 لديها سجلات بيانات اعتماد، و 73 لديها إدراجات حالية؛ وليس ذلك معدل انتشار وطنيًا
إذا تكرر حدث إقليمي كبير، فخطّط لموجة من ادعاءات DDoS من نشطاء القرصنة ضد المواقع الحكومية خلال أيام	متوسطة (افتراض تخطيطي)	ادّعت أربع مجموعات في مارس 2026، بدءًا خلال يوم واحد؛ الادعاءات غير مؤكدة؛ المؤشر: قوائم الأهداف في قنوات الجهات الفاعلة
إذا هيمنت أخبار التصعيد أو موضوعات الأزمات، فخطّط لطُعوم تجسس ضد الجهات الحكومية وقطاع الطاقة خلال يوم واحد	متوسطة (افتراض تخطيطي)	حملتان أبلغ عنهما مزودون في مارس 2026؛ عينة صغيرة؛ المؤشر: نشرات المزودين التحذيرية

الحكم	درجة الثقة	الأساس والحدود
خطّط لمزيد من ادعاءات البيانات التي تسمّي كبار أصحاب العمل وحائزي البيانات في قطر	متوسطة (افتراض تخطيطي)	ستة عشر عرضًا محددًا في 2026، تكرر اثنان منها؛ الأصالة غير متحقق منها؛ المؤشر: عروض جديدة في المنصات المرصودة
ستظل إدراجات مجموعات الفدية تسمّي المقاولين والموردين أكثر من الأسماء المعروفة	متوسطة بالنسبة للإدراجات المرصودة	9 إدراجات في 2026، معظمها لشركات متوسطة الحجم؛ الحوادث غير المنشورة غير مرئية

11.2 ما الذي قد يغيّر التقييم

التفسير الحالي	الأدلة التي قد تغيّره	القرار المتأثر
ادعاءات البيانات ضد جهات الطاقة والمصارف والأمن غير متحقق منها	عينة تطابق مخطط نظام محدد، أو تأكيد رسمي	تفعيل الإخطار وإجراءات حماية العملاء أو الموظفين لمجموعة البيانات تلك
أرقام نشطاء القرصنة تتجاوز ما أكده أي طرف	تأكيد رسمي لانقطاع مستمر في خدمة حيوية	إعادة النظر في قدرة التخفيف لدى مزود الخدمة الأعلى وخطط استمرارية الخدمة
الإدراجات الحالية تعني "تحقّق"، لا "اختُرق"	يُظهر التحقق أن بيانات اعتماد أو جلسة مدرجة لا تزال صالحة، أو يكشف وصولًا غير مصرّح به، سواء وُجدت MFA أم لا	التصعيد إلى الاستجابة للحوادث، وإلغاء الجلسات، وإعادة تعيين بيانات الاعتماد، وفرض MFA على الفئة المتأثرة
أدلة التجسس هي حملتان أبلغ عنهما مزودون	تقارير إضافية من مزودين أو جهات رسمية عن اختراقات في جهات حكومية أو جهات طاقة قطرية	تمويل أدوات رصد البريد ونقاط النهاية والهوية قبل المشاريع الأخرى
ادعاءات الفدية تسمّي في الغالب شركات متوسطة الحجم	إدراج يسمّي مشغّلًا للبنية التحتية الحيوية مع انقطاع مؤكد	إجراء اختبار الاستعادة الوارد في §12.1 أولًا ومراجعة صلاحيات وصول الموردين

11.3 سيناريوهات مشروطة

- **إذا** هيمن على الأخبار تصعيد إقليمي جديد أو حدث بارز يتعلق بقطر، **فعندئذٍ** خطّط لادعاءات DDoS ضد المواقع الحكومية واحتيال قائم على انتحال الهوية في الأسبوع نفسه. هذا افتراض تخطيطي، وليس فاصلًا زمنيًا مقيسًا؛ **المؤشر**: قوائم الأهداف في قنوات الجهات الفاعلة والتحذيرات الرسمية من الاحتيال. **القرار**: تفعيل خط التواصل المتفق عليه مسبقًا، والتخفيف لدى مزود الخدمة الأعلى، وتحذير العملاء من الاحتيال معًا.

- **إذا** كُشف عن ثغرة حرجة جديدة في منتج شبكي أو منتج للوصول عن بُعد، **فعندئذٍ** خطّط لمحاولات استغلال ضد الجهات الحكومية ومؤسسات الطاقة والاتصالات. **المؤشر:** نشرة تحذيرية من الوكالة الوطنية للأمن السيبراني تصنّف الثغرة على أنها مستغلة فعليًا. **القرار:** الترقيع والتحقق ضمن مهلة الترقيع لديك للأنظمة المكشوفة على الإنترنت، ثم البحث عن أصداف الويب (web shells).
- **إذا** ارتفع نشاط فحص البطاقات على نطاقات BIN الخاصة بك وأكد التحقيق أن بطاقات محددة يجري اختبارها، **فعندئذٍ** خطّط لمحاولات احتيال دون حضور البطاقة على تلك البطاقات. **المؤشر:** رفض متكتل لعمليات منخفضة القيمة من بوابات أجنبية. **القرار:** التحقيق في المحاولات، وفحص مؤشرات التفويض والاحتيال، وإعادة إصدار البطاقات المؤكد تعرضها للخطر.

الخلاصات الرئيسية

01

خطّط لأنواع الأدلة، لا لتهديد جديد: انكشاف الهوية، وهجمات DDoS المدفوعة بالأخبار، وطُعوم التجسس، وادعاءات البيانات المتكررة.

02

لكل حكم مؤشر؛ غيّر الخطة عندما يتغير المؤشر.

03

لا توجد بعد سلسلة زمنية قابلة للمقارنة للقول إن أيًا منها في تزايد.

الفصل 12

خطة العمل

يجيب هذا الفصل عن

ما الذي ينبغي أن يفعله كل فريق خلال الأيام الـ 90 المقبلة، وكيف سيعرف مجلس الإدارة أنه أُنجز؟

20
إجراءً لكل منها مالك ودليل إنجاز

في هذا الفصل

12.1 30/60/90 يومًا
12.2 حسب الدور
12.3 كيف يمكن أن تساعد Brandefense

باختصار

ابدأ بالتأكد من أنك تتلقى تنبيهات الإدراجات والأجهزة، ثم تصرّف بناءً على الأدلة الخاصة بك: إدراجات بيانات الاعتماد الحالية، وارتباطات أجهزة الموظفين، والرموز المكشوفة، ومرفقات البريد. ثم أغلق الثغرات المتعلقة بالتصيد الاحتيالي وموافقات الدفع والبريد الإلكتروني وDNS، وتدرّب على موجة DDoS مقترنة بادعاء تسريب بيانات. يعرف مجلس الإدارة أن العمل أُنجز من دليل الإنجاز في كل صف ومن بطاقة الأداء أدناه؛ قدّم كليهما بحلول اليوم 90.

12.1 30/60/90 يومًا

هذا تسلسل، وليس فترة انتظار. ينبغي أن يدخل أي تهديد جوهري حالي في عملية الاستجابة للحوادث لديك فورًا.

1 الأيام 1-30

2 الأيام 31-60

حيثما كانت سياسة DMARC على p=none أو غير موجودة، اجرد المرسلين وطبّق الإنفاذ تدريجيًا

المالك
فريق المراسلات

دليل الإنجاز
مرسلون متوافقون؛ p=quarantine مع مسار للتراجع

3 الأيام 61-90

وقّع DNS للنطاقات الرئيسية حيثما يدعم ذلك مسجّل النطاقات لديك؛ أصلح شهادات TLS غير الصالحة وأضف HSTS

المالك
فريقا الشبكات والويب

دليل الإنجاز
نجاح التحقق من DNSSEC من محلّل خارجي؛ اجتياز فحوص الشهادات

تأكد من أنك تتلقى تنبيهات إدراج بيانات الاعتماد للبيع والأجهزة المصابة لنطاقاتك الرئيسية؛ وإن لم يكن كذلك فرتّب ذلك؛ وإلى حين وصول التنبيهات، راجع عمليات تسجيل الدخول عن بُعد من أجهزة جديدة وافرض MFA على الوصول عن بُعد

المالك
مسؤول أمن المعلومات واستخبارات التهديدات

دليل الإنجاز
تسمية مصدر التنبيهات واستلام أول تنبيه، أو تسجيل مراجعة عمليات تسجيل الدخول وفرض MFA على الوصول عن بُعد

لكل إدراج حالي لبيانات اعتماد مرتبط بنطاقاتك، تحقّق من الحساب وحالة MFA الخاصة به خلال 5 أيام عمل

المالك
فريق الهوية

دليل الإنجاز
لكل إدراج قرار معالجة: إعادة تعيين، أو معالَج مسبقًا، أو لا يخصنا، مع التاريخ

تحقّق من ارتباطات الأجهزة المصنّفة كأجهزة موظفين؛ وألغِ الجلسات والرموز حيثما كانت نشطة

المالك
فريقا الهوية ونقاط النهاية

دليل الإنجاز
مطابقة قائمة الأجهزة مع جرد الأصول؛ تسجيل عمليات الإلغاء

احظر مرفقات الأرشيف والاختصارات الواردة من مرسلين خارجيين، وأطلق تنبيهًا عند تحميل برامج موقّعة لملفات DLL من مجلدات المستخدمين (§7.2)

المالك
فريق المراسلات ومركز العمليات الأمنية

دليل الإنجاز
تعديل سياسة البريد؛ اختبار التنبيه بعينة مصرّح بها

تعاقد على خدمة تخفيف DDoS لدى مزود الخدمة الأعلى أو اختبرها لبوابات المواطنين والعملاء وصفحات الدفع

المالك
البنية التحتية والمشتريات

دليل الإنجاز
سجل اختبار التخفيف

راجع الأدوار المميزة في الدليل، ومفاتيح السحابة في إعدادات التطبيقات، والحسابات على أنظمة أمن المباني (الحالة A)

المالك
الهوية والبنية التحتية

دليل الإنجاز
تسجيل المراجعة؛ إزالة الأدوار المميزة غير المستخدمة

راجع وصول الموردين عن بُعد، بما في ذلك مزودو أنظمة أمن المباني وإدارة المدارس

المالك
مخاطر الأطراف الثالثة

دليل الإنجاز
قائمة بصلاحيات وصول الموردين مع المالكين وتواريخ الانتهاء

انقل المستخدمين ذوي الصلاحيات المميزة والمستخدمين عن بُعد إلى MFA مقاومة للتصيد الاحتيالي (مفاتيح أمان FIDO2، أو مفاتيح المرور، أو تسجيل الدخول القائم على الشهادات)

المالك
فريق الهوية

دليل الإنجاز
تسجيل نسبة التغطية لكل مجموعة مستخدمين

فعّل رصد النطاقات المشابهة وانتحال الهوية لعلامتك التجارية، وانشر قنوات التواصل الحقيقية الخاصة بك

المالك
العلامة التجارية والاتصالات

دليل الإنجاز
تفعيل الرصد؛ نشر صفحة القنوات

أجرِ تمرينًا مكتبيًا يجمع بين موجة DDoS وادعاء متزامن بتسريب بيانات، بما في ذلك قرار الإبلاغ عن الحادثة الحرجة

المالك
مسؤول أمن المعلومات، والاتصالات، والشؤون القانونية

دليل الإنجاز
سجل القرارات والتوقيتات

قدّم بطاقة الأداء مقارنة بالمستهدفات (أدناه)

المالك
مسؤول أمن المعلومات إلى مجلس الإدارة

دليل الإنجاز
ورقة لمجلس الإدارة تتضمن الثغرات المتبقية ومالكيها

غيّر أي رمز تطبيق أو مفتاح أو كلمة مرور ظهرت في منشور علني أو عينة تسمّي مؤسستك (الحالة E)

المالك
مالكو التطبيقات

دليل الإنجاز
تسجيل التغيير؛ رفض القيم القديمة

سمِّ الشخص ونائبه اللذين يُبلغان الوكالة الوطنية للأمن السيبراني وجهة تنظيم الخصوصية، وبالنسبة للشركات المالية مصرف قطر المركزي أو مكتب مركز قطر للمال (10.3§)

المالك
مسؤول أمن المعلومات والشؤون القانونية

دليل الإنجاز
دليل إجراءات من صفحة واحدة يسمّي كل مهلة والمسؤول عن الإبلاغ عنها، معتمد

سمِّ المتحدث الرسمي والقناة المعتمدة لبيانات حالة الخدمة أثناء هجمات DDoS

المالك
الاتصالات

دليل الإنجاز
اعتماد نماذج البيانات

اشترط تأكيدًا عبر قناة مستقلة لتغييرات تعليمات الدفع والمستفيدين، بما في ذلك الطلبات التي تستشهد بجهة رسمية

المالك
المالية ومكافحة الاحتيال

دليل الإنجاز
اعتماد الإجراء؛ ضبط طلب محاكى واحد

أضف MFA وتنبيهات الاسترداد إلى حسابات الولاء وحسابات العملاء

المالك
الفرق الرقمية وفرق مكافحة الاحتيال

دليل الإنجاز
تفعيل التنبيه؛ تسجيل نسبة تغطية MFA

أطلق تنبيهًا عند رفض متكتل لعمليات فحص البطاقات على نطاقات BIN الخاصة بك

المالك
مكافحة الاحتيال

دليل الإنجاز
تفعيل التنبيه؛ تسجيل أول مراجعة

أجرِ اختبار استعادة موقوتًا لنظام واحد من الأنظمة الأكثر أهمية

المالك
البنية التحتية

دليل الإنجاز
تسجيل زمن الاستعادة مقارنة بهدف زمن الاستعادة (RTO: أطول انقطاع تسمح به خطة استمرارية الأعمال لديك)

مستهدفات بطاقة الأداء. هذه قيم افتراضية مقترحة؛ حدّد قيمك الخاصة حيثما اختلفت السياسة.

المقياس	المستهدف
الإدراجات الحالية التي اتُّخذ بشأنها قرار معالجة خلال 5 أيام عمل	100% بحلول اليوم 90
الأجهزة المصنّفة كأجهزة موظفين المطابَقة مع جرد الأصول	100% بحلول اليوم 90

المقياس	المستهدف
حظر مرفقات الأرشيف والاختصارات الخارجية	مطبّق بحلول اليوم 30
النطاقات الرئيسية التي تطبّق DMARC على quarantine أو reject	100%، أو خطة مؤرخة، بحلول اليوم 90
المستخدمون ذوو الصلاحيات المميزة والمستخدمون عن بُعد على MFA مقاومة للتصيد الاحتيالي	100%، أو خطة مؤرخة، بحلول اليوم 90
تغييرات المستفيدين وتعليمات الدفع المؤكدة عبر قناة مستقلة	100% بحلول اليوم 90
اختبار الاستعادة ضمن RTO	ناجح، أو إصلاح مؤرخ، بحلول اليوم 90
رصد إدراجات بيانات الاعتماد للبيع والأجهزة المصابة للنطاقات الرئيسية، داخليًا أو عبر مزود	مطبّق بحلول اليوم 30

يوفر التمرين السيبراني الوطني موعدًا جاهزًا للتدريب: حددت الوكالة الوطنية للأمن السيبراني موعد تمرينها الثالث عشر (13) في 30 نوفمبر 2026، بمشاركة أكثر من 150 جهة في 14 قطاعًا [S40].

12.2 حسب الدور

الدور	القرار الأول
مجلس الإدارة	اطلب أعداد الإدراجات الحالية وأجهزة الموظفين الخاصة بمؤسستك والتاريخ الذي يُتحقق فيه من كل منها، وتأكد من وجود الرصد الذي ينتجها
مسؤول أمن المعلومات	طبّق رصد الإدراجات والأجهزة أولًا، ثم ضوابط المرفقات ودليل إجراءات مهل الإبلاغ
مركز العمليات الأمنية	أضف قواعد كشف لتنفيذ ملفات الأرشيف والاختصارات، وللملفات الثنائية الموقّعة التي تحمّل ملفات DLL من مجلدات المستخدمين، ولإشارات Cobalt Strike، ولعمليات تسجيل الدخول من أجهزة جديدة إلى VPN وسطح المكتب البعيد
مكافحة الاحتيال	استخدم مؤشرات مخاطر الجهاز والجلسة عند تسجيل الدخول وتغيير المستفيدين؛ وراقب الرفض المتكتل لعمليات فحص البطاقات على نطاقات BIN الخاصة بك؛ وحذّر العملاء من انتحال صفة الجهات الحكومية

الدور	القرار الأول
الاتصالات	جهّز بيانات الحالة الخاصة بهجمات DDoS وبادعاءات التسريب غير المتحقق منها، مع الفصل بين الادعاء والحقيقة المتحقق منها والإجراء

الخلاصات الرئيسية

01

تأكد من الرصد، ثم تحقّق من الإدراجات الحالية وأجهزة الموظفين واحظر مرفقات الأرشيف الخارجية خلال أول 30 يومًا.

02

طبّق DMARC وMFA المقاومة للتصيد الاحتيالي وضوابط تغيير الدفع تدريجيًا بحلول اليوم 60؛ وقدّم بطاقة الأداء بحلول اليوم 90.

03

تدرّب على موجة DDoS مقترنة بادعاء تسريب بيانات، بما في ذلك قرار الإبلاغ عن الحادثة الحرجة.

12.3 كيف يمكن أن تساعد Brandefense

تجمع Brandefense بين استخبارات التهديدات السيبرانية، وحماية المخاطر الرقمية، وإدارة سطح الهجوم الخارجي. واستخدم التحليل في هذا التقرير البيانات وآلية التقييم ذاتها التي تطبّقها المنصة على المؤسسات المرصودة: ارتباطات الأجهزة المصابة وبيانات الاعتماد، وإدراجات أسواق بيانات الاعتماد الحالية، والنطاقات المشابهة، والمستندات المكشوفة، والإشارات على الويب المظلم. ولا يَعِد بإمكانية التحقق من كل ادعاء أو بأن يظل أي سجل تاريخي صالحًا للاستخدام.

أحضر نطاقاتك وعلاماتك التجارية وأولوياتك الأمنية إلى عرض توضيحي مدته 30-45 دقيقة مع فريقي المبيعات وما قبل البيع. ويمكن للفريق أن يوضح كيف يربط رصد المنصة الإشارات الخارجية بالأصول التي تديرها. وسيتابع معك أحد أعضاء فريق Brandefense أو شريك في منطقتك.

اطلب عرضًا توضيحيًا

الملحق A. المنهجية

A.1 النافذة الزمنية والمصادر والأولوية

تمتد نافذة البحث من 1 يناير إلى 20 نوفمبر 2026 بحسب تاريخ نشر المنشور، لا تاريخ جمعه. تأتي بياناتنا الخاصة أولاً: Brandefense Blackhole (منشورات الويب المظلم وتطبيقات المراسلة، وارتباطات الأجهزة المصابة وبيانات الاعتماد، ومواد البطاقات الواردة في المنشورات)، وRansompedia (إدراجات مواقع التسريب لدى مجموعات الفدية)، وتصنيفات التعرض في Brandefense Atlas. توفر المصادر الخارجية السياق، ولا يُستشهد بها إلا بعد قراءة المقطع الداعم. استُخرجت البيانات في 21 نوفمبر

2026. المصادر S1–S6 وS8 هي بيانات خاصة بـ Brandefense وليس لها عنوان عام؛ ويحمل كل مصدر خارجي في الملحق C رابطاً وتاريخ فتحنا له.

A.2 منشورات Blackhole

البند	القيمة
المنشورات التي تحمل وسم دولة قطر	55,241
المنشورات بعد التنقية	7,867–8,175 (نطاق، لا تقدير نقطي)

تُستبعد الرسائل المزعجة والمنشورات الآلية قبل التحليل. وكثير من المنشورات المتبقية قوائم متعددة الدول، لذا تبقى الأعداد بعد التنقية حداً أعلى للنشاط الإجرامي المتعلق بقطر.

ثلاثة قيود في الجمع تشكّل كل اتجاه في هذا التقرير. لا نقارن فئات المنشورات على امتداد العام. ويبدو الجمع أقل منذ منتصف العام، لذا لا نقرأ الانخفاضات على أنها اتجاهات في التهديد. وبعض المنشورات التي تذكر قطر لا صلة لها بالموضوع: منشورات عن بنك تركي، ومنشورات تستخدم كلمة "قطر" بمعناها الآخر "القُطر" (diameter).

A.3 المؤسسات الـ 250

الاختيار والتحقق والقيود مبيّنة في §3.1. لكل نطاق رئيسي قرأنا إشارات التعرض التي يستخدمها Atlas في تصنيفاته. وهي: الأجهزة المصابة، وأجهزة الموظفين، وسجلات بيانات الاعتماد، والإشارات في محادثات الويب المظلم والويب المظلم، والنطاقات المشابهة الجديدة، والمستندات التي تشير إلى النطاق، والإدراجات الحالية والسابقة في أسواق بيانات الاعتماد. قُرئت أعداد الأجهزة وبيانات الاعتماد والإدراجات في 21 نوفمبر 2026.

A.4 تصنيفات Atlas

حصلت كل مؤسسة على تصنيف تعرض من Atlas استناداً إلى هذه الإشارات، وحصلت القائمة كلها على درجة رئيسية واحدة. تعامل مع الإدراج الحالي في سوق بيانات الاعتماد على أنه سبب للتحقق من الحسابات، لا دليلاً على اختراق.

A.5 فحوص DNS وTLS والويب

أجرينا استعلامات DNS عامة لسجلات البريد وSPF وDMARC وDKIM وDNSSEC، إضافة إلى فحص TLS وفحص للصفحة الرئيسية لكل نطاق. تُحتسب سياسات DMARC المفقودة وغير الصالحة وتلك المقتصرة على المراقبة (p=none) على أنها بلا إنفاذ. لم يتجاوز أي فحص هذه الفحوص السلبية.

مؤشر النظافة السلبي هو مركّب تحليلي من Odin لهذه الفحوص الخاصة بالبريد الإلكتروني وDNS وTLS والترويسات، على مقياس من 0-100. تعني القيمة الأعلى نظافة أضعف؛ وهو نموذج، لا تصنيف من Atlas.

A.6 مواد البطاقات في المنشورات

النطاق: بطاقات الدفع التي ظهرت بنص واضح في منشورات الويب المظلم التي جُمعت لهذا التقرير فقط. تكتشف Brandefense البطاقات المسروقة عبر طرق أخرى كثيرة تقع خارج هذا التقرير. لا تقيس هذه الأرقام سرقة البطاقات أو خسائر الاحتيال.

لا تُورد سوى أعداد إجمالية حسب الجهة المُصدرة؛ ولا تُنشر أي بيانات بطاقات.

A.7 برامج الفدية

استخدمنا الإدراجات المقبولة في Ransompedia لقطر والإمارات العربية المتحدة والمملكة العربية السعودية والكويت والبحرين، لجميع التواريخ، مؤرخة بحسب تاريخ النشر. يُستخدم متتبع عام ومنشورات Blackhole المنقولة للتحقق المتقاطع فقط.

A.8 تغطية الحوادث

قورنت الحوادث الواردة في هذا التقرير ببيانات Blackhole وبالتقارير العامة، بما يشمل الصحافة الوطنية والصفحات الرسمية للجهات الحكومية وأبحاث الموردين وحسابات الرصد العامة.

قيود التغطية المتبقية. لا تزال رؤيتنا جزئية:

- لا تُغطّى مواقع تسريب برامج الفدية على شبكة Tor إلا عبر Ransompedia.
- تقع المنتديات المغلقة والمقتصرة على الدعوات، ومجموعات Telegram الخاصة، والمبيعات التي تُرتّب عبر الرسائل المباشرة خارج نطاق جمعنا.
- المنشورات المحذوفة قبل الجمع مفقودة.
- قد تُساء قراءة اللهجات العربية والعامية.
- تعذّرت القراءة المباشرة لعدة مواقع رسمية وصحفية، ولأجزاء من الصحافة الناطقة بالعربية.
- تبقى الحوادث التي تعالجها المؤسسات دون إفصاح غير مرئية.

غياب حادثة عن هذا التقرير لا يعني أنها لم تقع.

A.9 الثقة والحدود

تنطبق الثقة العالية على قياس قابل للتكرار، لا على الادعاء الأساسي لمجرم. وتشير الثقة المتوسطة إلى تفسير له سند داعم واضح وقيود مذكورة. وتعني عبارة "غير متحقق منه" أنه لم يُثبت بشكل مستقل؛ وهي ليست دليلاً على التلفيق ولا دليلاً على اختراق. تُوصف المؤسسات الضحية بحسب دورها؛ ولا تُسمّى جهة حكومية أو شركة إلا حيث يؤكد بيان رسمي الحادثة وحيث نُشر عنها على نطاق واسع. تُطبع الأسماء البديلة للجهات الفاعلة؛ وتُحجب الروابط وجهات الاتصال والمؤشرات والبيانات الشخصية. يُحتفظ بالمصدر الكامل في سجل أدلة داخلي.

الملحق B. سجل الأدلة

يظهر كل منشور مقتبس في هذا التقرير على شكل بطاقة منشور منقّحة في الفصل المبيّن. المقتطفات قصيرة؛ والمحذوفات مُعلّمة بـ [...]؛ وتُستبدل المعرّفات وجهات الاتصال والروابط والرموز والعينات والمؤسسات الضحية بتسميات بين أقواس، وفق السياسة الواردة في A.9. الترجمات من عملنا ما لم يحمل المنشور نص الجهة الفاعلة نفسها بالإنجليزية. تواريخ النشر ليست تواريخ الاختراق. يُحتفظ بمعرّفات المنشورات وروابطها ونصوصها الكاملة في سجل أدلة داخلي.

البطاقة	تاريخ النشر	المنصة	الاسم البديل كما يظهر	اللغة	يظهر في
B01	2026-02-19	منتدى اختراقات	ناشر غير مسمّى	الإنجليزية	4.4§
B02	2026-03-10	قناة Telegram	ELIPHAS SYNDICATE	الإنجليزية	4.4§
B03	2026-03-10	منتدى اختراقات	TheAshborn	الإنجليزية	4.4§
B04	2026-11-10	منتدى اختراقات	UNC6783 (تسمية ذاتية)	الإنجليزية	4.5§
B05	2026-08-26	قناة Telegram ناقلة لإدراج من منتدى	قناة ناقلة لأخبار الأمن	الإنجليزية	4.5§
B06	2026-06-08	منتدى اختراقات	ناشر غير مسمّى	الإنجليزية	4.5§
B07	2026-09-03	منتدى	ناشر غير مسمّى	الإنجليزية	4.5§
B08	2026-09-03	منتدى، والنص نفسه على Telegram	مشترٍ مجهول	الإنجليزية	4.5§

البطاقة	تاريخ النشر	المنصة	الاسم البديل كما يظهر	اللغة	يظهر في
B09	2026-03-03	قناة الجهة الفاعلة	Keymous Plus	الإنجليزية، كما نُشرت	6.3§
B10	2026-03-12	قناة الجهة الفاعلة	Keymous Plus	الإنجليزية، كما نُشرت	6.2§
B11	2026-03-14	قناة الجهة الفاعلة	Team 313	العربية، مع نص المجموعة نفسها بالإنجليزية	6.2§
B12	2026-03-06	قناة ناقلة لروبوت تتبع آلي	DieNet (منقول)	الإنجليزية	6.3§
B13	2026-06-19	قناة الجهة الفاعلة	BD Anonymous Team	الإنجليزية، كما نُشرت	6.3§
B14	2026-01-01	قناة متجر لحسابات الولاء	متجر أميال	الإنجليزية	8.3§
B15	2026-03-24	قناة الجهة الفاعلة	Keymous Plus	الإنجليزية، كما نُشرت	6.3§
B16	2026-07-22	قناة Telegram ناقلة لإدراج من منتدى	قناة ناقلة لأخبار الأمن	الإنجليزية	4.4§
B17	2026-03-09	قناة Telegram	بائع بيانات	العربية، مع نص البائع نفسه بالروسية والإنجليزية	4.4§
B18	2026-05-16	منتدى	ناشر غير مسمّى	الإنجليزية	4.5§

الملحق C. المصادر

S1 منشورات Brandefense Blackhole المتعلقة بقطر، تواريخ النشر من 1 يناير إلى 20 نوفمبر 2026، استُخرجت في 21 نوفمبر 2026.

S2 منشورات Brandefense Blackhole من قنوات ناشطي القرصنة (هاكتفيست) والقنوات الناقلة التي تسمّي أهدافاً قطرية، من 28 فبراير إلى 19 يونيو 2026.

S3 ارتباطات Brandefense Blackhole بالأجهزة المصابة وقواعد بيانات الاختراقات وسجلات برامج سرقة المعلومات وقوائم الدمج (combolist) لـ 250 نطاقاً، كما كانت محفوظة في 21 نوفمبر 2026.

S4 تصنيفات Brandefense Atlas للانكشاف وإشاراته للنطاقات الـ 250، 21 نوفمبر 2026، بما في ذلك إدراجات أسواق بيانات الاعتماد والنطاقات المشابهة والمستندات المكشوفة والإشارات.

S5 فحوص Brandefense العامة لـ DNS وTLS والصفحات الرئيسية للـ 250 نطاقاً، 21 نوفمبر 2026.

S6 Brandefense Ransompedia، الإدراجات المقبولة لقطر والإمارات العربية المتحدة والمملكة العربية السعودية والكويت والبحرين، لجميع التواريخ، استُخرجت في 21 نوفمبر 2026.

S7 ransomware.live، ضحايا الدولة لرمز QA، تم الوصول إليه في 21 نوفمبر 2026 (للتحقق المتقاطع فقط). https://www.ransomware.live/ (رابط المقال محجوب). تم التحقق في 21 نوفمبر 2026.

S8 Brandefense Blackhole، أعداد إجمالية للبطاقات المرتبطة بقطر التي ظهرت بنص واضح في المنشورات المجمّعة، 21 نوفمبر 2026.

S9 DataReportal (Kepios)، *Digital 2027: Qatar*، 5 نوفمبر 2026 (بيانات أكتوبر 2026). https://datareportal.com/reports/digital-2027-qatar. تم التحقق في 21 نوفمبر 2026.

S10 Qatar News Agency (وكالة الأنباء القطرية)، "Qatar achieves one of the world's highest scores in ITU ICT Development Index 2026"، 24 أغسطس 2026، نقلاً عن هيئة تنظيم الاتصالات. https://qna.org.qa/en/News-Area/News/2026-8/24/qatar-achieves-one-of-the-worlds-highest-scores-in-itu-ict-development-index-2026. تم التحقق في 21 نوفمبر 2026.

S11 US Energy Information Administration (إدارة معلومات الطاقة الأمريكية)، موجز التحليل القُطري لقطر، آخر تحديث في 20 أكتوبر 2025. https://www.eia.gov/international/analysis/country/QAT. تم التحقق في 21 نوفمبر 2026.

S12 Hamad International Airport (مطار حمد الدولي)، بيان صحفي عن الأداء التشغيلي لعام 2025، 21 يناير 2026. https://dohahamadairport.com/press-releases/news/2025-operational-performance. تم التحقق في 21 نوفمبر 2026.

S13 مصرف قطر المركزي (Qatar Central Bank)، "Retail Payment Systems" (صفحة غير مؤرخة). https://www.qcb.gov.qa/en/Pages/Retail-payment-systems.aspx. تم التحقق في 21 نوفمبر 2026.

S14 القرار الأميري رقم (1) لسنة 2021 بإنشاء الوكالة الوطنية للأمن السيبراني، بتاريخ 14 مارس 2021، الجريدة الرسمية 24 مارس 2021. النص الرسمي على بوابة الميزان (Al Meezan): https://almeezan.qa/legislations/16ffa013-351b-4a84-8b03-7752c25ce4f1. تم التحقق في 21 نوفمبر 2026.

S15 الوكالة الوطنية للأمن السيبراني (National Cyber Security Agency)، الاستراتيجية الوطنية للأمن السيبراني 2024-2030 (الصفحة ووثيقة الاستراتيجية). https://www.ncsa.gov.qa/en/national-cyber-security-strategy. تم التحقق في 21 نوفمبر 2026.

S16 الوكالة الوطنية للأمن السيبراني، المعيار الوطني لضمان أمن المعلومات، الإصدار 2.1، مايو 2023. https://www.ncsa.gov.qa/en/publications (مكتبة الوثائق). فُتحت صفحة المكتبة في 21 نوفمبر 2026؛ ولم يُؤكَّد نص الوثيقة في هذا الإصدار.

S17 الوكالة الوطنية للأمن السيبراني، الإطاران الوطني والمؤسسي لإدارة مخاطر أمن المعلومات، الإصدار 1.0 (2026). وكذلك ضوابطها للمشاركين في الأسواق المالية، الإصدار 1.0 (مارس 2026). https://www.ncsa.gov.qa/en/publications (مكتبة الوثائق). فُتحت صفحة المكتبة في 21 نوفمبر 2026؛ ولم يُؤكَّد نص الوثيقة في هذا الإصدار.

S18 الوكالة الوطنية للأمن السيبراني، "NCSA Organizes the Fifth Annual Cyber Governance and Assurance Conference"، 5 أكتوبر 2026. https://www.ncsa.gov.qa/en/media/news/x-551750. تم التحقق في 21 نوفمبر 2026.

S19 القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية، بتاريخ 15 سبتمبر 2014، الجريدة الرسمية 2 أكتوبر 2014. النص الرسمي على بوابة الميزان (Al Meezan): https://almeezan.qa/legislations/71b9f8f2-61dc-44b9-825d-b16c490ed583. تم التحقق في 21 نوفمبر 2026.

S20 القانون رقم (11) لسنة 2025 بتعديل بعض أحكام قانون مكافحة الجرائم الإلكترونية، بتاريخ 21 يوليو 2025، الجريدة الرسمية 4 أغسطس 2025. النص الرسمي على بوابة الميزان (Al Meezan): https://almeezan.qa/legislations/2af771cb-8553-4a91-ab94-1f6fede99cf9. تم التحقق في 21 نوفمبر 2026.

S21 القانون رقم (13) لسنة 2016 بشأن حماية خصوصية البيانات الشخصية، بتاريخ 3 نوفمبر 2016، الجريدة الرسمية 29 ديسمبر 2016. النص الرسمي على بوابة الميزان (Al Meezan): https://almeezan.qa/legislations/9c7dca4b-8722-4212-9368-ea3abba0c95c. وقُرئت مواد العقوبات في النص الإنجليزي الصادر عن الوكالة الوطنية للأمن السيبراني، الذي تصفه بأنه غير رسمي، وفي صفحتها الخاصة بقانون حماية خصوصية البيانات الشخصية (PDPPL) https://www.ncsa.gov.qa/en/pages/personal-data-privacy-protection-law. تم التحقق في 21 نوفمبر 2026.

S22 الوكالة الوطنية للأمن السيبراني، "Personal Data Breach Notifications: Guidelines for Regulated Entities"، الإصدار 2.0، سبتمبر 2022. https://www.ncsa.gov.qa/en/pages/personal-data-breach-notification. تم التحقق في 21 نوفمبر 2026.

S23 مصرف قطر المركزي، لائحة الحوسبة السحابية (Cloud Computing Regulation)، صادرة في أبريل 2024. https://www.qcb.gov.qa/Documents/InformationSecurity/Cloud%20Computing%20Regulation.pdf. تم التحقق في 21 نوفمبر 2026.

S24 مركز قطر للمال (Qatar Financial Centre)، مكتب حماية البيانات، "Data Protection Regulations and Rules 2021 Guidance" وصفحة حماية البيانات ونموذج الإبلاغ عن الاختراق (المادة 31). https://www.qfc.qa/en/operate/data-protection/ و https://www.qfc.qa/media/stxham4h/qfc_data_protection_breach_reporting_form.pdf. تم التحقق في 21 نوفمبر 2026.

S25 Gulf Times، "National Cyber Security Agency takes action against sports sector firm over data breach"، 3 فبراير 2026. https://www.gulf-times.com/article/719867/qatar/national-cyber-security-agency-takes-action-against-. تم التحقق في 21 نوفمبر 2026.

S26 Check Point Research، "China-nexus activity against Qatar observed amid expanding regional tensions"، 9 مارس 2026. https://blog.checkpoint.com/research/china-nexus-activity-against-qatar-observed-amid-expanding-regional-tensions/. تم التحقق في 21 نوفمبر 2026.

S27 Check Point Research، تقرير استخبارات التهديدات الأسبوعي (Threat Intelligence Report)، 16 مارس 2026. https://research.checkpoint.com/2026/16th-march-threat-intelligence-report/. تم التحقق في 21 نوفمبر 2026.

S28 Palo Alto Networks Unit 42، "Threat Brief: Escalation of Cyber Risk Related to Iran"، محدّث في 17 أبريل 2026. https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/. تم التحقق في 21 نوفمبر 2026.

S29 CloudSEK، تقرير وضع عن التصعيد في الشرق الأوسط والنشاط السيبراني، 2 مارس 2026. https://www.cloudsek.com/blog/middle-east-escalation-israel-iran-us-cyber-war-2026. تم التحقق في 21 نوفمبر 2026.

S30 Intel 471، تدوينة عن الارتفاع الحاد في نشاط ناشطي القرصنة (هاكتفيست) بعد بدء التصعيد الإقليمي، 9 مارس 2026. https://www.intel471.com/blog/israeli-us-strikes-against-iran-triggers-a-surge-in-hacktivist-activity. تم التحقق في 21 نوفمبر 2026.

S31 StormWall، "Q1 2026 DDoS report: MENA" (صفحة غير مؤرخة). https://stormwall.network/resources/blog/q1-2026-ddos-report-mena. تم التحقق في 21 نوفمبر 2026.

S32 NETSCOUT، تقرير استخبارات التهديدات (Threat Intelligence Report)، صفحة دولة قطر، يناير–يونيو 2026. https://www.netscout.com/threatreport/country/qatar/. تم التحقق في 21 نوفمبر 2026.

S33 The National، "Iranian cyber attacks move from disruptive to complex threats in Gulf"، 10 أبريل 2026. https://www.thenationalnews.com/future/technology/2026/04/10/iranian-cyber-attacks-move-from-disruptive-to-complex-threats-in-gulf/. تم التحقق في 21 نوفمبر 2026.

S34 DailyDarkWeb، تقرير عن هجوم DDoS الذي ادّعته DieNet ضد مواقع حكومية قطرية (يسمّي العنوان الجهات)، 6 مارس 2026. https://dailydarkweb.net/ (رابط المقال محجوب). تم التحقق في 21 نوفمبر 2026.

S35 Gulf Times (QNA)، "Ministry of Interior warns against calls exploiting ongoing situation"، 24 مارس 2026. https://www.gulf-times.com/article/722806/qatar/ministry-of-interior-warns-against-calls-exploiting. تم التحقق في 21 نوفمبر 2026.

S36 Qatar Tribune، "GTA issues urgent warning over scam messages impersonating officials"، 26 فبراير 2026. https://www.qatar-tribune.com/article/221421/business/gta-issues-urgent-warning-over-scam-messages-impersonating-officials. تم التحقق في 21 نوفمبر 2026.

S37 Gulf Times، "Blackmailing can lead to 3-year jail term, QR100,000 fine, MoI official warns"، 28 سبتمبر 2026. https://www.gulf-times.com/article/734377/qatar/blackmailing-can-lead-to-3-year-jail-term-qr100000-fine-moi-official-warns. تم التحقق في 21 نوفمبر 2026.

S38 Gulf Times، "National Cyber Security Agency Urges Immediate iPhone Security Update for Users in Qatar"، 22 مارس 2026. https://www.gulf-times.com/article/722733/qatar/national-cyber-security-agency-urges-immediate-iphone-security-update-for-users-in-qatar. تم التحقق في 21 نوفمبر 2026.

S39 Gulf Times، "CRA launches updated Qatar Domains Registry policies to strengthen digital security and trust"، 3 نوفمبر 2026. https://www.gulf-times.com/article/737448/qatar/cra-launches-updated-qatar-domains-registry-policies. تم التحقق في 21 نوفمبر 2026.

S40 Qatar News Agency (وكالة الأنباء القطرية)، مقابلة مع رئيس لجنة التمارين السيبرانية الوطنية بشأن التمرين السيبراني الوطني رقم 13، 15 نوفمبر 2026. https://qna.org.qa/en/News-Area/News/2026-11/15/cyber-exercises-committee-head-to-qna-national-drill-to-test-institutional-preparedness-for-cyber-incidents. تم التحقق في 21 نوفمبر 2026.

S41 Gulf Times، "Qatar financial system demonstrates strong resilience in 2025: QCB"، 3 أغسطس 2026. https://www.gulf-times.com/article/730424/business/qatar-financial-system-demonstrates-strong-resilience-in-2025-qcb. تم التحقق في 21 نوفمبر 2026.

S42 Microsoft Learn، "List of Azure regions" (محدّث في 17 نوفمبر 2026)، و Google Cloud، "Regions and zones". https://learn.microsoft.com/en-us/azure/reliability/regions-list و https://docs.cloud.google.com/compute/docs/regions-zones. تم التحقق في 21 نوفمبر 2026.

S43 الوكالة الوطنية للأمن السيبراني، قائمة النشرات الاستشارية للأمن السيبراني (Cybersecurity Advisories)، من 1 يناير إلى 20 نوفمبر 2026. https://www.ncsa.gov.qa/en/media/cybersecurity-advisories. تم التحقق في 21 نوفمبر 2026.

S44 Proofpoint، "Iran conflict drives heightened espionage activity against Middle East targets"، 11 مارس 2026. https://www.proofpoint.com/us/blog/threat-insight/iran-conflict-drives-heightened-espionage-activity-against-middle-east-targets. تم التحقق في 21 نوفمبر 2026.

S45 Marhaba، "NCSA Warns Public About Rise in Phishing and Impersonation Scams"، 19 سبتمبر 2026. https://marhaba.qa/ncsa-warns-public-about-rise-in-phishing-and-impersonation-scams/. تم التحقق في 21 نوفمبر 2026.

S46 Silent Push، تقرير عن 10 Smishing Triad، 2025 أبريل. https://www.silentpush.com/blog/smishing-triad/. تم التحقق في 21 نوفمبر 2026.

S47 Al Jazeera، "Israeli ad-tech firm helped place spyware on Al Jazeera devices"، 15 أكتوبر 2026، نقلًا عن نتائج Citizen Lab. https://www.aljazeera.com/news/2026/10/15/israeli-ad-tech-firm-helped-spy-on-al-jazeera-devices. تم التحقق في 21 نوفمبر 2026.

S48 Citizen Lab (Bill Marczak وآخرون)، "Exposing AdFection: How Discover-Tech Turned Targeted Ads Into a Pipeline for Zero-Click Mercenary Spyware"، 15 أكتوبر 2026. https://citizenlab.ca/research/how-discover-tech-turned-targeted-ads-into-a-pipeline-for-spyware/. تم التحقق في 21 نوفمبر 2026.

الملحق D. مسرد المصطلحات

- **Blackhole**: مصدر بيانات الجرائم السيبرانية لدى Brandefense، ويغطي المنشورات والأجهزة المصابة وبيانات الاعتماد ومواد البطاقات.
- **Ransompedia**: قاعدة بيانات برامج الفدية لدى Brandefense؛ تسجّل الإدراجات ادعاءات إجرامية.

- **Atlas**: نظام Brandefense لتقييم التعرض الخارجي؛ تتراوح الدرجات من 0 (لم يُرصد شيء) إلى 100.
- **جهاز مصاب**: جهاز يحتوي سجل برنامج سرقة المعلومات الخاص به على تسجيل دخول إلى نطاق المؤسسة؛ و"جهاز الموظف" جهاز مصنّف بوصفه جهازًا لأحد الموظفين، دون التحقق من التوظيف.
- **إدراج في سوق بيانات الاعتماد**: بيانات اعتماد مرتبطة بالنطاق معروضة في سوق خاضع للرصد وقت الفحص.
- **قائمة دمج (combolist)**: قائمة بأزواج أسماء الدخول وكلمات المرور مجمّعة من مصادر مختلفة؛ ويتفاوت عمرها وصلاحيتها.
- **سجل برنامج سرقة المعلومات**: بيانات التقطتها برمجية خبيثة لسرقة المعلومات من جهاز.
- **روبوت فحص (Checker bot)**: روبوت يختبر البطاقات المسروقة على بوابات الدفع ويطبع النتيجة.
- **بطاقة منشور**: نسخة منقّحة من منشور واحد على الويب المظلم، مع المنصة والتاريخ والاسم البديل واللغة وما يثبته المنشور وما لا يثبته.
- **قناة ناقلة / نقل**: قناة أو روبوت تابع لطرف ثالث يعيد نشر ادعاء جهة فاعلة أخرى؛ والنقل دليل أضعف من منشور الجهة الفاعلة نفسها.
- **رابط فحص التوافر**: رابط إلى خدمة عامة تختبر ما إذا كان موقع ويب يستجيب من عدة مواقع؛ وهو يسجّل لحظة، لا انقطاعاً.
- **منتدى الاختراقات**: منتدى تُعرض فيه البيانات المسروقة وصلاحيات الوصول إلى الشبكات وتُتداول.
- **مُسيِّل البطاقات (card casher)**: مجرم يحوّل بيانات البطاقات المسروقة إلى مال أو سلع.
- **المحمّل (في الاحتيال)**: مجرم يشحن الحسابات أو يدفع الفواتير ببطاقات مسروقة مقابل نسبة؛ أما في §7.2 فيعني "المحمّل" مرحلة من برمجية خبيثة.
- **الدردشات المظلمة**: قنوات مراسلة مغلقة، مثل مجموعات Telegram، تُستخدم في التجارة الإجرامية.
- **روبوت OTP**: خدمة آلية تتصل بالضحايا أو تراسلهم لخداعهم كي يكشفوا كلمة مرور لمرة واحدة.
- **تضخيم DNS**: أسلوب DDoS يرسل استعلامات DNS صغيرة بعنوان مصدر مزوّر لتُغرق الإجاباتُ الكبيرة الهدف.
- **احتيال البطاقة غير الحاضرة (card-not-present)**: مدفوعات عبر الإنترنت أو الهاتف تُنفَّذ ببيانات بطاقة مسروقة وحدها.
- **Web shell**: نص برمجي خبيث يوضع على خادم ويب ويمنح المهاجم تحكمًا فيه عن بُعد.
- **خدمة إغراق مأجورة (stresser)**: خدمة DDoS مأجورة، تُباع غالباً على أنها "اختبار إجهاد".
- **متجر أميال**: قناة تبيع حسابات ولاء شركات الطيران والفنادق، غالباً مع إمكانية الوصول إلى صندوق البريد المرتبط.
- **DMARC / SPF / DKIM**: معايير مصادقة البريد الإلكتروني؛ يبلغ DMARC الجهات المستقبلة بما يجب فعله بالبريد الذي يفشل في المصادقة.
- **DNSSEC**: تواقيع تتيح للمحلّلات التحقق من إجابات DNS.
- **سجل DS**: السجل في المنطقة الأم الذي يربط النطاق بمفاتيح DNSSEC الخاصة به.
- **HSTS**: ترويسة ويب تبلغ المتصفحات باستخدام HTTPS فقط.

- **TLP:CLEAR**: يجوز مشاركته دون قيود؛ وتظل الالتزامات القانونية الأخرى سارية.
- **PlugX / Cobalt Strike**: عائلة برمجيات خبيثة للوصول عن بُعد استُخدمت طويلاً في التجسس، وأداة تجارية لمحاكاة الهجمات يستخدمها المجرمون والجواسيس أيضاً.
- **اختطاف DLL**: جعل برنامج مشروع يحمّل مكتبة خبيثة موضوعة في المكان الذي يبحث فيه البرنامج أولاً.
- **BIN**: بادئة رقم البطاقة الخاصة بالجهة المُصدرة (رقم تعريف البنك).
- **KYC**: فحوص التحقق من الهوية "اعرف عميلك" لدى البنوك ومنصات التداول والخدمات الأخرى.
- **MFA (المصادقة متعددة العوامل)**: تسجيل دخول يتطلب عاملاً ثانياً إضافة إلى كلمة المرور.
- **MFA المقاومة للتصيد**: تسجيل دخول مرتبط بالموقع الحقيقي (مفاتيح أمان FIDO2 أو مفاتيح المرور أو الشهادات)، بحيث لا تستطيع صفحة نقل وسيطة إعادة استخدامه.
- **الدرجة الرئيسية**: درجة Atlas الملخّصة على المستوى الوطني لجميع المؤسسات الـ 250.
- **مؤشر النظافة السلبي**: مركّب تحليلي من Odin لفحوص البريد الإلكتروني وDNS وTLS والترويسات؛ من 0–100، والقيمة الأعلى تعني أضعف.
- **NCSA**: الوكالة الوطنية للأمن السيبراني في قطر، وهي السلطة السيبرانية الوطنية والجهة المنظِّمة لخصوصية البيانات الشخصية.

عن هذا التقرير

أعدّه Odin by Brandefense. اكتمل الإصدار 1.0 في 21 نوفمبر 2026.

تاريخ انتهاء البحث: 20 نوفمبر 2026 (نافذة البيانات الأساسية). يمنح التقرير الأولوية لبيانات Brandefense الخاصة، ويفصل الادعاءات الإجرامية عن الحوادث المثبتة بشكل مستقل، ولا يدّعي إحصاءً كاملاً للجرائم السيبرانية التي تطال قطر. تصف التوصيات ما يمكن للمؤسسات فعله؛ ولا تقرر أن أي مؤسسة قد فعلته أو لم تفعله. تُنشر طبعة باللغة العربية من الإصدار 1.0 بالتوازي مع الطبعة الإنجليزية؛ وتكون الغلبة للطبعة الإنجليزية عند وجود أي اختلاف بينهما.

© 2026 Brandefense. جميع الحقوق محفوظة.