تقرير Brandefense عن مشهد التهديدات السيبرانية في الإمارات العربية المتحدة 2026

انكشاف الهوية، وسوق لحسابات المقيمين، وادعاءات تدميرية خلال فترة الأزمة في اقتصاد خليجي عالي الرقمنة

TRANSLATED WITH AI

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

إعداد
Odin by Brandefense

نُشر
21 نوفمبر 2026

مدة القراءة
88 دقيقة للقراءة

النسخة
الإصدار 1.0 · Public Research Edition · TLP:CLEAR

فترة البحث
1 يناير–20 نوفمبر 2026

109 من 250
مؤسسة كانت لديها بيانات اعتماد مُدرجة للبيع يوم الفحص

130,477
منشوراً مصنّفاً على أنه يتعلق بدولة الإمارات، 1 يناير–20 نوفمبر 2026

10
ادعاءات DDoS في منشورات الجهات الفاعلة التي قرأناها ضد أهداف إماراتية، جميعها بين 2 مارس و 8 أبريل

12 من 23
مصرفاً في قائمتنا لديها بيانات اعتماد مدرجة للبيع يوم الفحص

المحتويات

01 الملخص التنفيذي
02 السياق الرقمي وسياق التهديدات في الإمارات العربية المتحدة
04 ما نرصده على الويب المظلم
06 نشاط ناشطي القرصنة وهجمات حجب الخدمة الموزعة (DDoS) والادعاءات التدميرية
08 اقتصاد الاحتيال
خريطة التقرير
03 الانكشاف الوطني: 250 مؤسسة رائدة
05 أمثلة على الاستهداف بحسب القطاع
07 الجهات الفاعلة في التهديد
09 نظرة معمّقة على القطاع 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 للمؤسسات في الإمارات، وما الذي ينبغي أن يقرره القادة أولاً؟

4

قرارات للقادة، يستند كل منها إلى أدلة في الفصول

في هذا الفصل

أربعة قرارات للقادة
العام بالأرقام

باختصار

بالنسبة إلى المؤسسات الرائدة الـ 250 في الإمارات التي قيّمناها، يتمثل الانكشاف الرئيسي المقاس في الهوية: ارتباطات بأجهزة مصابة وبيانات اعتماد، وبيانات اعتماد مُدرجة للبيع لدى 109 منها. وتتاجر السوق السرية بحسابات موثّقة للمقيمين في الإمارات وببيانات عقارية طوال العام. وتركّزت ادعاءات الهجمات التدميرية وهجمات حجب الخدمة الموزعة (DDoS) ضد أهداف حكومية وأهداف في قطاعي الطاقة والنقل في مارس وأبريل، ولم تؤكدها الجهات المذكورة. اعملوا بهذا الترتيب: تحققوا من الإدراجات، ثم اختبروا استعادة النسخ الاحتياطية، ثم عزّزوا ضوابط فتح الحسابات.

يجمع هذا التقرير بين ثلاثة من مصادر بيانات Brandefense الخاصة وتقارير عامة جرى التحقق منها. قدّم **Brandefense** عدد 130,477 منشوراً موسوماً بأنه يتعلق بالإمارات، و 1,271 منشوراً مميزاً في المنتديات تذكر الإمارات. كما قدّم سجلات **Blackhole** الأجهزة المصابة وبيانات الاعتماد لـ 250 مؤسسة مختارة، وبيانات بطاقات ظهرت بنص واضح في المنشورات. وقدّم **Ransompedia** إدراجات مواقع التسريب الخاصة ببرامج الفدية للإمارات ولأربع دول خليجية للمقارنة. واحتُسبت تقييمات الانكشاف من **Atlas** للمؤسسات الـ 250. هذه مجموعات منفصلة، ولا تُجمع معاً في أي موضع.

1. **تطال ارتباطات بيانات الاعتماد والأجهزة المصابة كل المؤسسات الرائدة تقريباً.** لدى 234 من المؤسسات الـ 250 أجهزة مصابة مرتبطة بنطاقاتها (522,128 جهازاً على الأقل في المجموع). ومعظمها (491,713) غير مصنّف أجهزةً للموظفين، والأرجح أن كثيراً منها أجهزة يملكها مقيمون وعملاء، وإن لم تثبت ملكيتها؛ ومنها 30,415 مصنّفة أجهزةً للموظفين. ولدى 241 منها سجلات تاريخية لبيانات الاعتماد (1,856,314 سجلاً). تشمل هذه الأعداد جميع السجلات المحفوظة في 21 نوفمبر 2026 أياً كان تاريخ التقاطها، فهي تراكمية وليست مقتصرة على 2026. وقد تخص موظفين أو طلاباً أو مقيمين أو عملاء. هذه أعداد ارتباطات: أما معرفة ما إذا كان أي حساب لا يزال صالحاً للدخول، ولمن يعود، فتتطلب التحقق. [S2][S3]

2. **كانت لدى 109 من 250 مؤسسة بيانات اعتماد مُدرجة للبيع وقت الفحص.** يمنح Atlas المؤسسات الـ 250 تقييماً رئيسياً وطنياً قدره 53 على مقياس من 0 إلى 100، حيث يعني 0 عدم رصد أي مخاطر؛ وهو تقييم موجز، لا متوسط. يدلّ الإدراج المدافع على ضرورة البحث عن حساب نشط، لكنه لا يحدد عدد الحسابات ولا أصحابها. [S3]

3. **تركّزت ادعاءات الهجمات التدميرية وهجمات DDoS خلال الأزمة وبقيت غير مؤكدة.** وقعت ادعاءات ناشطي القرصنة (هاكتيفست) في منشورات الجهات الفاعلة التي قرأناها بشنّ هجمات DDoS على مواقع اتحادية ومحلية بين 2 مارس و 8 أبريل. وادّعت Handala، وهي علامة تصفها Security Affairs بأنها يُنظر إليها على نطاق واسع كواجهة لجهة مدعومة من إيران، تنفيذ هجمات ببرمجيات المسح التدميرية (wiper) وسرقة بيانات لدى عدة جهات من القطاع العام في إحدى الإمارات. وبلغت الأحجام التي ادّعتها 6 PB من البيانات المُتلفة و 149 TB من البيانات المسروقة. ولم تؤكد الجهات المذكورة ولا السلطات هذه الادعاءات حتى تاريخ الإغلاق لدينا. وقد حذّرت الجهة الوطنية المعنية بالأمن السيبراني نفسها في أبريل من حملة إقليمية نشطة لبرمجيات المسح التدميرية. [S1][S11][S26]

4. **تصدّرت حسابات المقيمين وبيانات العقارات العروض الإماراتية، وتجاوزت إدراجات الفدية نظيراتها الخليجية.** أكثر المواضيع الخاصة بالإمارات استمراراً هو تداول حسابات مصرفية وحسابات محافظ وتحويلات وصرافة مرتبطة ببطاقة الهوية الإماراتية أو بطاقة الإقامة، إلى جانب تجنيد الحسابات الوسيطة لتمرير الأموال (mule). وكانت بيانات ملاك العقارات والمستأجرين والبوابات العقارية أكثر فئات البيانات الخاصة بالإمارات عرضاً في المنشورات التي راجعناها، من تسعة بائعين على الأقل. ويُدرج Ransompedia عدد 84 إدراجاً لبرامج الفدية في الإمارات خلال الفترة، وهو أعلى بكثير من السعودية (30) وقطر (9) وعُمان (9) والكويت (7). [S1][S5]

5. **قلّة من الحوادث في التقارير العامة التي راجعناها حظيت بتأكيد مفصّل.** وصف رئيس مجلس الأمن السيبراني لحكومة دولة الإمارات مختترقاً استغل ثغرة غير مُعالَجة لدى مؤسسة من القطاع الخاص وطالب بمبلغ 5 ملايين USD. وفي نوفمبر أكدت Landmark Group وصولاً غير مصرح به إلى برنامج الولاء Shukran ربما كُشفت فيه الأسماء وبيانات الاتصال وتواريخ الميلاد، وذلك بعد يوم من إدراج مجموعة تدير موقع تسريب للشركة. وبصورة منفصلة، أفادت شركات أمنية بعمليات تجسس مرتبطة بدول استهدفت جهات إماراتية عبر صناديق بريد مُستولى عليها وإغراءات بعروض عمل. [S17][S67][S24][S31][S32]

أربعة قرارات للقادة

1. **تعاملوا مع الإدراجات الحالية لبيانات الاعتماد بوصفها مُحفّزاً لحادث، لا رقماً إحصائياً.** وجّهوا كل إدراج حالي في السوق مرتبط بنطاقاتكم إلى فريق الهوية. احتووا في اليوم نفسه الحسابات ذات الصلاحيات المميزة أو الوصول عن بُعد أو التي تفتقر إلى المصادقة متعددة العوامل (MFA)، وسجّلوا قراراً بشأن البقية خلال 5 أيام عمل. ورتّبوا مراقبة إدراجات بيانات الاعتماد والأجهزة المصابة الخاصة بنطاقاتكم اعتباراً من اليوم 1، عبر فريق داخلي أو مزوّد خدمة (§12.1؛ الصفان 1-2).
2. **أثبتوا قدرتكم على التعافي من برمجيات المسح التدميرية.** تصف نشرة المجلس نفسها برمجيات خبيثة تدميرية تدخل عبر التصيّد الاحتيالي وبيانات اعتماد VPN المسروقة والأنظمة غير المحدَّثة. استعيدوا نظاماً حيوياً من نسخة احتياطية غير متصلة خلال الوقت المتعهَّد به، وحدّثوا أنظمة الأطراف الشبكية المنتهي دعمها أو اعزلوها (§6.4؛ §12.1؛ الصفان 4 و6).
3. **استعدوا لادعاءات تسبق الحقائق.** اتفقوا مسبقاً على الجهة التي تؤكد حالة الخدمة علناً خلال حملات ناشطي القرصنة، ورتّبوا مسبقاً للتخفيف من هجمات DDoS على مستوى المزوّد للبوابات العامة قبل فترة التصعيد المقبلة (§12.1؛ الصفان 9 و16).

4. **اكسروا سلسلة الاحتيال على الحسابات.** إن التحقق من هوية العميل (KYC) ببطاقة الإقامة والحسابات الوسيطة لتمرير الأموال والاستيلاء عبر الوصول عن بُعد حلقات في سلسلة واحدة. انقلوا الموافقات بعيداً عن رموز الرسائل النصية، واختبروا فتح الحسابات واستردادها بحالات اصطناعية (§8، §10.3؛ §12.1 الصفان 10 و18).

العام بالأرقام

130,477

منشورات في Blackhole موسومة بأنها تتعلق بالإمارات، 1 يناير–20 نوفمبر 2026

ما لا يمثله

ليس عدداً للهجمات؛ يضم أكتوبر وحده 32,435 منشوراً، معظمها من عائلة واحدة من روبوتات تداول الحسابات

23,663–24,456

منشورات ذات صلة في الفترة يناير–يوليو ونوفمبر، تُعرض نطاقاً (من أصل 65,544 منشوراً موسوماً)

ما لا يمثله

ليست حوادث فريدة؛ من بين 30 منشوراً عشوائياً ذا صلة، ذكر 10 فقط الإمارات تحديداً

250

مؤسسة رائدة من القطاعين العام والخاص قُيّمت بمنهجية Atlas

ما لا يمثله

ليست عينة عشوائية؛ وليست تقديراً لمعدل الانتشار الوطني

522,128+

جهازاً مصاباً مرتبطاً بنطاقات المؤسسات الـ 250 (30,415 مصنّفة أجهزةً للموظفين)؛ تراكمي، يشمل جميع السجلات المحفوظة في 21 نوفمبر 2026

ما لا يمثله

ليس مقتصراً على 2026، ولا يمثل أفراداً فريدين، ولا إصابات حالية مؤكدة؛ حدّ أدنى

109 من 250

مؤسسة لديها بيانات اعتماد مُدرجة للبيع وقت الفحص

ما لا يمثله

ليس عدداً للحسابات ولا لاختراقات مؤكدة

84

إدراجاً مقبولاً لبرامج الفدية في Ransompedia يخص الإمارات بتاريخ 1 يناير–20 نوفمبر 2026 (74 مؤسسة إماراتية مميزة محتملة)

ما لا يمثله

ليست عمليات اختراق مؤكدة؛ الإدراجات ادعاءات إجرامية

128

حادثاً عدّتها الجهة الوطنية المعنية بالأمن السيبراني مؤكدة حتى 18 فبراير 2026

ما لا يمثله

غير قابل للمقارنة مع أعدادنا؛ مجموعة ومنهجية مختلفتان

10

ادعاءات لناشطي القرصنة بشنّ هجمات DDoS في منشورات الجهات الفاعلة التي قرأناها، جميعها بين 2 مارس و 8 أبريل

ما لا يمثله

ليست انقطاعات مؤكدة

631

بطاقة دفع مميزة مرتبطة بالإمارات ظهرت بنص واضح في منشورات الويب المظلم التي جمعناها (504 منها منسوبة إلى جهة إصدار إماراتية مسماة)

ما لا يمثله

ليس رقماً لخسائر الاحتيال؛ نطاق ضيق (§8.2)

82%

من المؤسسات الـ 250 تطبّق (204) DMARC

ما لا يمثله

ليس مقياساً لنجاح التصيّد الاحتيالي

خريطة التقرير

اثنا عشر فصلاً وخمسة مسارات للقراءة. ابدأوا بالصف الذي يطابق دوركم. يبدأ كل فصل بالسؤال الذي يجيب عنه، وتُختتم الفصول 2-12 بثلاث خلاصات.

مجلس الإدارة والتنفيذيون

ماذا حدث، وما مدى انكشافنا، وما الذي ينبغي أن نقرّره؟

انتقل إلى 1 3 12

كبير مسؤولي أمن المعلومات وقادة الأمن

أيّ أشكال الانكشاف تخصّنا، وأيّ الجهات الفاعلة مهمة، وأيّ الضوابط تأتي أولاً؟

انتقل إلى 3 6 7 9 10 12

مركز العمليات الأمنية واستخبارات التهديدات

ماذا نشرت الجهات الفاعلة، وكيف ترتبط ببعضها، وما التقنيات المستخدمة في التجسس؟

انتقل إلى 4 6 7 8 12

الملحقان A-B

الاحتيال وحماية العملاء

كيف تُتداول الهويات والحسابات والبطاقات الإماراتية، وأين ترى البنوك ذلك؟

انتقل إلى 4 5 8 9

الاتصال المؤسسي والشؤون القانونية

كيف نتحدث عن الادعاءات غير المؤكدة، وما قواعد الإخطار المنطبقة؟

انتقل إلى 6 10 12

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

02 **السياق**
أيّ خصائص الإمارات تشكّل صورة التهديدات فيها

03 **الانكشاف الوطني**
كيف تُقيَّم 250 مؤسسة رائدة وفق منهجية Atlas

04 **الويب المظلم**
ما الذي ينشره المجرمون عن الإمارات بعد إزالة الرسائل المزعجة

05 **القطاعات**
أيّ القطاعات تُذكر بالاسم، وما الاستجابة التي يحتاجها كل منها

06 **نشاط ناشطي القرصنة**
ما الذي ادُّعي، وما الذي قيل رسمياً، وكيف نستعد

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

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

09 **القطاع المصرفي**
أين يتركّز الانكشاف الظاهر للبنوك

10 **التنظيم**
أيّ القواعد تنطبق، وما الذي تغيّر في 2026

11 **التوقعات**
ما الذي ينبغي التخطيط له، وما الذي قد يغيّر الخطة

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

الفصل 2

السياق الرقمي وسياق التهديدات في الإمارات العربية المتحدة

يجيب هذا الفصل عن

ما السمات التي تشكّل صورة التهديدات السيبرانية في الإمارات في 2026، وماذا أعلنت السلطات الوطنية؟

99%

نسبة انتشار الإنترنت (الحد الأقصى لدى المصدر)، مع 23.0 مليون اشتراك خلوي

في هذا الفصل

2.1 سكان متصلون يعتمدون على الهاتف المحمول أولاً

2.2 هوية رقمية وحكومة مركزيتان

2.3 أزمة إقليمية وأرقام الهجمات الرسمية

2.4 التصريحات الرسمية بشأن الإسناد

باختصار

ثلاث سمات تشكّل صورة التهديدات في الإمارات: اتصال شبه شامل يعتمد على الهاتف المحمول أولاً؛ ونموذج مركزي للهوية الرقمية؛ وأزمة إقليمية بدأت أواخر فبراير. وقد ربطتها الجهة الوطنية المعنية بالأمن السيبراني بارتفاع حاد في محاولات الهجوم. تصف الأرقام الرسمية حجم الضغط لا النتائج. خطّطوا للتصدي للبرمجيات الخبيثة التدميرية والاحتيال على الهوية في آن واحد: اختبروا النسخ الاحتياطية غير المتصلة وعزّزوا ضوابط استرداد الحسابات.

2.1 سكان متصلون يعتمدون على الهاتف المحمول أولاً

أحصت DataReportal 11.4 مليون نسمة في أكتوبر 2025، و 11.3 مليون مستخدم للإنترنت في نهاية 2025، أي بنسبة انتشار 99.0% (تحدّ DataReportal نسبة الاستخدام عند 99%). كما أحصت 23.0 مليون اشتراك خلوي، أي 202% من عدد السكان، و 12.5 مليون هوية مستخدم على وسائل التواصل الاجتماعي، وقد لا تمثل أفراداً فريدين [S8].

يترتب على ذلك أمران للمدافعين. يصل الاحتيال الموجّه إلى المقيمين في الإمارات بلغات عديدة: فالمنشورات الإجرامية التي نحتفظ بها عن الإمارات مكتوبة في معظمها بالإنجليزية والروسية، وحصة العربية منها صغيرة (الفصل 4). كما أن أرقام الهواتف المحمولة وتطبيقات المراسلة والخدمات المصرفية عبر التطبيقات هي القنوات الرئيسية لتقديم الخدمات وللاحتيال معاً.

2.2 هوية رقمية وحكومة مركزيتان

تعتمد الإمارات هوية رقمية وطنية موحّدة هي UAE PASS، وقد أفادت وكالة أنباء الإمارات الرسمية (WAM) بأن عدد مستخدميها المسجلين تجاوز 12 مليوناً [S55]. وتقع خلفها البوابات الاتحادية والمحلية. تجعل الهوية المركزية الخدمات أسرع، لكنها تركّز القيمة أيضاً: فجلسة UAE PASS صالحة أو نسخة من وثيقة هوية تفتح أبواباً كثيرة. وفي مارس حذّرت شرطة دبي من متصلين ينتحلون صفة موظفي إدارة الأزمات للحصول على بيانات UAE PASS وبطاقة الهوية الإماراتية بهدف تبديل شرائح SIM والاستيلاء على تطبيقات المصارف [S49].

يقود مجلس الأمن السيبراني لحكومة دولة الإمارات، الذي أُنشئ بقرار من مجلس الوزراء في نوفمبر 2020 [S54]، السياسة السيبرانية الوطنية. واعتمد مجلس الوزراء الاستراتيجية الوطنية للأمن السيبراني الحالية في 3 فبراير 2025، وهي تقوم على خمس ركائز: الحوكمة، والحماية، والابتكار، وبناء القدرات، والشراكة [S43]. وفي يونيو 2026 أُعلن عن هيئة اتحادية جديدة للذكاء الاصطناعي والبيانات، تجمع بحسب تحليل لإحدى شركات المحاماة الإشراف على الذكاء الاصطناعي والحكومة الرقمية وتنظيم البيانات [S41]. ويبيّن الفصل 10 ما يعنيه ذلك للمؤسسات.

2.3 أزمة إقليمية وأرقام الهجمات الرسمية

أفاد رئيس المجلس بفترة تصعيد في النشاط السيبراني من 28 فبراير حتى أوائل أبريل 2026، خلال ما وصفه بالأزمة الإقليمية [S22]. وفي أوائل مارس أفاد قسم الحوسبة السحابية لدى Amazon بنشوب حريق في مركز بيانات في الإمارات بعد أن أصابت أجسامٌ المنشأة، ما أثّر في توافر الخدمة. كان ذلك الانقطاع مادياً وليس هجوماً سيبرانياً. وتعذّر الوصول إلى بعض الخدمات المصرفية عبر الإنترنت والهاتف في اليوم نفسه، والسبب غير معلن [S29].

نشر المجلس أرقاماً على مدار العام. وهي مستمدة من مناسبات وفترات وصياغات مختلفة، ولم ينشر المجلس منهجية لها، لذا لا تشكّل سلسلة زمنية. وفي 21 أكتوبر شدّد المجلس نفسه على أن ارتفاع عدد المحاولات المرصودة «لا يشير بالضرورة» إلى زيادة في الاختراقات الناجحة [S20].

التاريخ	ما قاله المجلس	المصدر
2026-02-18	128 حادثاً مؤكداً منذ 1 يناير؛ 90,000-200,000 محاولة اختراق يومياً	[S9]
2026-02-21	إحباط هجمات منظمة «ذات طابع إرهابي» على المنصات الوطنية: محاولات اختراق الشبكات وبرامج الفدية والتصيّد الاحتيالي	[S10]
2026-04-01	ارتفاع الهجمات اليومية من نحو 200,000 إلى نحو 600,000	[S13]
2026-04-20	نحو 800,000 هجوم يومياً خلال الهدنة، مقابل نحو 200,000 قبل الأزمة	[S14]

التاريخ	ما قاله المجلس	المصدر
2026-07-03	أكثر من 800,000 محاولة يومياً؛ إحباط هجمات على جهات في القطاع المالي	[S15]
2026-08-10	التصدي لهجمات متقدمة ومنظمة على قطاعات الطيران والطاقة والتعليم	[S16]
2026-09-15	تسجيل 640,000 هجوم في يوم واحد	[S17]
2026-10-21	إحباط نحو 750,000 محاولة «في الأشهر الأخيرة»	[S20]
2026-10-28	معالجة الفرق الوطنية لثغرة واسعة الانتشار في PHP؛ ولم يُذكر رقم CVE	[S21]
2026-11-18	أكثر من 40 مجموعة من أكثر من 20 دولة حاولت استغلال الأزمة	[S22]

يمثل تفصيل فبراير أنفع خط أساس رسمي. من بين الحوادث المؤكدة الـ 128، صنّف المجلس 38.3% منها تشويهاً للمواقع الإلكترونية، و 25.8% تسريباً للبيانات، و 13.3% اختراقاً للبيانات، و 10.2% وصولاً أولياً، و 7.8% برامج فدية، و 4.7% هجمات DDoS. وحمل Telegram نسبة 49.2% من النشاط ذي الصلة، والويب المفتوح 40.6%، ومواقع Tor نسبة 10.2%. وكان القطاع الحكومي (9.4%) والخدمات المالية (9.3%) أكثر القطاعات تضرراً [S9]. ويغلب Telegram أيضاً على ما نجمعه نحن (99.6% من المنشورات الموسومة)؛ أما فيما عدا ذلك فالمزيج الرسمي وعائلات منشوراتنا يقيسان أشياء مختلفة ولا نقارن بينهما.

2.4 التصريحات الرسمية بشأن الإسناد

تفاوتت التصريحات الرسمية حول الجهات التي تقف وراء النشاط بحسب المناسبة. نسجّلها كما نُقلت، من دون إسناد من جانبنا.

التاريخ	التصريح كما نُقل	المصدر
2026-02-18	قال المجلس إن «نسبة كبيرة» من الهجمات نفّذتها مجموعات تهديد متقدمة مدعومة من دول. وإن 15 من أصل 21 مجموعة تهديد متقدمة (APT) مرصودة مدعومة من دول. ورصد المجلس أيضاً 60 جهة من ناشطي القرصنة والمجرمين	[S9]
2026-04-20	عدّد رئيس المجلس مجموعات من بينها، بحسب ما أُفيد، مجموعات ذات صلات بإيران	[S14]
2026-09-16	في مقابلة مع CNN نقلتها The National، سمّى رئيس المجلس إيران والحرس الثوري الإيراني (IRGC، Islamic Revolutionary Guard Corps)	[S18]
2026-09-17	كتبت Euronews أن المسؤول نفسه لم ينسب العمليات إلى أي دولة	[S19]

التاريخ	التصريح كما نُقل	المصدر
2026-11-18	في القمة العالمية للشرطة، سمّى رئيس المجلس إيران وشبكات مرتبطة بالحرس الثوري ضمن أكثر من 40 منظمة	[S23]

ما يعنيه ذلك للمدافعين. لا يغيّر الجدل حول الإسناد الضوابط المطلوبة. فتحذيرات المجلس نفسه تصف برمجيات المسح التدميرية والتصيّد الاحتيالي وبيانات اعتماد VPN المسروقة والأنظمة غير المحدَّثة المكشوفة على الإنترنت بوصفها نقاط الدخول [S11]. وهي الضوابط نفسها أياً كانت الجهة المشغّلة.

الخلاصات الرئيسية

01

الاتصال شبه الشامل والهوية الرقمية المركزية يجعلان بيانات الهوية والجلسات الغنيمة الأثمن.

02

تقيس أرقام الهجمات الرسمية المحاولات على أسس مختلفة؛ اقرؤوها مؤشراً على الضغط لا اتجاهاً.

03

تحدد نشرات المجلس نفسه نقاط الدخول: التصيّد الاحتيالي وبيانات اعتماد VPN وأنظمة الأطراف الشبكية غير المحدَّثة.

الفصل 3

الانكشاف الوطني: 250 مؤسسة رائدة

يجيب هذا الفصل عن

ما مدى انكشاف المؤسسات الرائدة الـ 250 من القطاعين العام والخاص في الإمارات عند تقييمها بالطريقة التي يقيّم بها Brandefense Atlas العميل، وأي إشارة ينبغي للمدافع فرزها أولاً؟

109 من 250

مؤسسة كانت لديها بيانات اعتماد مُدرجة للبيع يوم الفحص

في هذا الفصل

3.1 بطاقة المجموعة المدروسة
3.2 التقييم الوطني والإدراجات الحالية بحسب القطاع
3.3 الأجهزة وبيانات الاعتماد
3.4 الإدراجات الحالية لبيانات الاعتماد
3.5 النطاقات الشبيهة والوثائق المكشوفة والإشارات
3.6 سلامة البريد الإلكتروني والمواقع

باختصار

قيّمنا 250 مؤسسة رائدة في الإمارات باستخدام تقييمات الانكشاف في Brandefense Atlas. لدى جميعها تقريباً أجهزة مصابة وسجلات بيانات اعتماد مرتبطة بنطاقاتها، وكانت لدى 109 منها بيانات اعتماد مُدرجة للبيع وقت فحصنا. أما سلامة البريد الإلكتروني فقوية نسبياً: إذ تطبّق 204 من 250 مؤسسة DMARC. ويندر استخدام DNSSEC. ابدؤوا بفرز الإدراجات الحالية، ثم أجهزة الموظفين، ثم مخازن بيانات الاعتماد الكبيرة في الجامعات والجهات الحكومية.

3.1 بطاقة المجموعة المدروسة

البند	التعريف
المجموعة	250 مؤسسة: 68 جهة حكومية، و 35 في المصارف والتمويل، و 19 في الطاقة والمرافق، و 19 في النقل والخدمات اللوجستية، و 18 في التعليم، و 16 في التجزئة والشركات القابضة، و 11 في التأمين، و 11 في التكنولوجيا، و 11 في الرعاية الصحية، و 10 في العقارات والإنشاءات، و 9 في التصنيع والصناعة، و 9 في الضيافة والسياحة، و 8 في الإعلام، و 6 في الاتصالات. منها 184 حكومية أو مرتبطة بالحكومة، و 60 خاصة، و 6 أجنبية

البند	التعريف
الاختيار	اختيار هادف: جهات وبوابات اتحادية ومحلية، ومصارف وشركات دفع مرخّصة من المصرف المركزي، ومؤسسات مرتبطة بالحكومة، وشركات رائدة في السوق. اختيرت بحسب الحجم أو الدور النظامي، ولم تُرتّب بحسب الإيرادات؛ ولم يُستخدم أي تصنيف منشور لأكبر 250 مؤسسة في الإمارات
الوحدة	نطاق رئيسي واحد لكل مؤسسة. جميع النطاقات الـ 250 تُحلّ في DNS (21 نوفمبر 2026). بالنسبة إلى 173 نطاقاً، قُرئت الصفحة الرئيسية لتأكيد الملكية؛ أما النطاقات الـ 77 الأخرى فتعذّرت قراءتها ونُسبت بمطابقة النطاق مع الاسم الرسمي للمؤسسة. واستُبعد 68 من أصل 318 مرشحاً لكونها مكررة أو خارج النطاق أو غير مطابقة لمؤسستها
القياسات	الأجهزة المصابة وأجهزة الموظفين، وسجلات قواعد بيانات الاختراقات وسجلات برمجيات سرقة المعلومات وقوائم combolist، والإشارات في محادثات ومنتديات الويب المظلم، والنطاقات الشبيهة، والوثائق المكشوفة، والإدراجات الحالية في أسواق بيانات الاعتماد، باستخدام البيانات نفسها التي يستخدمها Atlas؛ إضافة إلى فحوص عامة لـ DNS وTLS وترويسات HTTP
التاريخ	قُرئت الأعداد في 21 نوفمبر 2026. تشمل أعداد الأجهزة وبيانات الاعتماد والإدراجات جميع السجلات المحفوظة في ذلك التاريخ، بصرف النظر عن تاريخ الالتقاط (تراكمية، وليست مقتصرة على 2026). تغطي أعداد الإشارات 365 يوماً حتى 18 نوفمبر 2026؛ وتغطي أعداد النطاقات الشبيهة آخر 30 يوماً
من دون إزالة التكرار	عبر المصادر أو عبر المؤسسات أو عبر الأفراد. قد يظهر الشخص الواحد في عدة مصادر؛ وقد يحتوي الجهاز الواحد على بيانات دخول لعدة مؤسسات
غير تمثيلية	تصف النتائج هذه القائمة. وهي ليست معدلات انتشار وطنية

3.2 التقييم الوطني والإدراجات الحالية بحسب القطاع

يقيّم Atlas كل مؤسسة من 0 (لا مخاطر مرصودة) إلى 100. ويمنح Atlas المؤسسات الـ 250 تقييماً رئيسياً وطنياً قدره 53 على هذا المقياس من 0 إلى 100؛ وهو تقييم موجز، لا متوسط. ويعرض التقرير أعداد الإشارات بحسب القطاع.

كيف تُقرأ تقييمات Atlas.

المصطلح	المعنى
الرقم الرئيسي	التقييم الموجز الوطني الذي يعرضه Atlas؛ وهو ليس متوسطاً
الإدراج الحالي	بيانات اعتماد مرتبطة بالنطاق معروضة للبيع وقت الفحص
سجل الإدراجات	عُرضت بيانات اعتماد مرتبطة بالنطاق للبيع في وقت سابق

كانت لدى 205 مؤسسات مطابقات مرشّحة لنطاقات شبيهة؛ ولم يُتحقَّق من جميع هذه المطابقات.

بيانات الاعتماد والأجهزة المصابة شائعة في كل قطاع؛ وتتفاوت الإدراجات الحالية بين 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 والترفيه (8)	62%	75%	62%	62%	88%	75%	100%
التكنولوجيا (11)	82%	100%	55%	55%	100%	91%	91%
الحكومة (68)	59%	85%	53%	54%	96%	75%	94%
الاتصالات (6)	33%	83%	50%	50%	100%	67%	67%
المصارف والتمويل (35)	66%	94%	37%	46%	100%	83%	100%
التعليم (18)	78%	89%	44%	44%	100%	100%	100%
الضيافة والسياحة (9)	56%	78%	44%	44%	100%	44%	89%
التجزئة والشركات القابضة (16)	81%	69%	38%	44%	100%	75%	100%
النقل والخدمات اللوجستية (19)	58%	79%	32%	42%	95%	79%	89%
الرعاية الصحية (11)	55%	64%	36%	36%	100%	82%	100%
التأمين (11)	36%	73%	27%	27%	100%	82%	100%
التصنيع والصناعة (9)	56%	56%	11%	22%	78%	78%	89%
الطاقة والمرافق (19)	53%	79%	16%	21%	89%	84%	84%
العقارات والإنشاءات (10)	70%	80%	10%	20%	100%	70%	80%

المصدر: ارتباطات Brandefense Blackhole ومنهجية Atlas لـ 250 مؤسسة، قُرئت في 21 نوفمبر 2026 [S2][S3]. السجلات تراكمية، وليست خاصة بعام 2026 وحده.

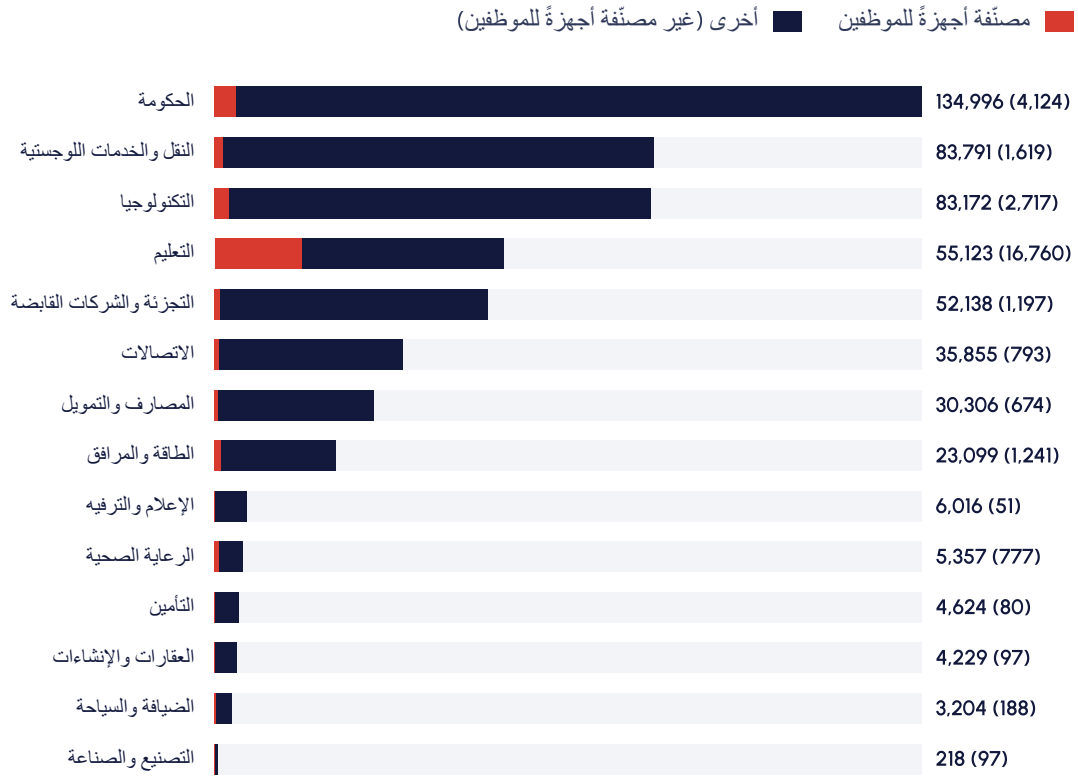
القطاع	المؤسسات	مؤسسات لديها إدراج حالي لبيانات الاعتماد
الحكومة	68	37
المصارف والتمويل	35	16
الطاقة والمرافق	19	4
النقل والخدمات اللوجستية	19	8
التعليم	18	8

القطاع	المؤسسات	مؤسسات لديها إدراج حالي لبيانات الاعتماد
التجزئة والشركات القابضة	16	7
التأمين	11	3
التكنولوجيا	11	6
الرعاية الصحية	11	4
العقارات والإنشاءات	10	2
التصنيع والصناعة	9	2
الضيافة والسياحة	9	4
الإعلام والترفيه	8	5
الاتصالات	6	3
جميع المؤسسات الـ 250	**250**	**109**

قراءة الجدول. ابدأوا الفرز من عمود الإدراجات. ولدى الحكومة (37 من 68) والمصارف والتمويل (16 من 35) أكبر عدد من المؤسسات ذات الإدراج الحالي. وفي الإعلام (5 من 8) والاتصالات (3 من 6) والتكنولوجيا (6 من 11) النصف أو أكثر مُدرج، لكن القطاعات الثلاثة صغيرة.

3.3 الأجهزة وبيانات الاعتماد

تحمل قطاعات الحكومة والنقل والتكنولوجيا أكبر عدد من ارتباطات الأجهزة المصابة؛ وتضم الجامعات معظم الأجهزة المصنّفة أجهزةً للموظفين



المصدر: ارتباطات Brandefense Blackhole ومنهجية Atlas لـ 250 مؤسسة، قُرئت في 21 نوفمبر 2026 [S2][S3]. السجلات تراكمية، وليست خاصة بعام 2026 وحده.

القطاع	مؤسسات لديها أجهزة مصابة	الأجهزة (الموظفون)	سجلات بيانات الاعتماد	حصة بيانات الاعتماد لدى أكبر
الحكومة	64 من 68	134,996 (4,124)	157,226	57%
النقل والخدمات اللوجستية	17 من 19	83,791 (1,619)	232,300	63%
التكنولوجيا	10 من 11	83,172 (2,717)	92,414	71%
التعليم	18 من 18	55,123 (16,760)	958,690	58%
التجزئة والشركات القابضة	16 من 16	52,138 (1,197)	65,414	60%

القطاع	مؤسسات لديها أجهزة مصابة	الأجهزة (الموظفون)	سجلات بيانات الاعتماد	حصة بيانات الاعتماد لدى أكبر
الاتصالات	4 من 6	35,855 (793)	38,288	94%
المصارف والتمويل	35 من 35	30,306 (674)	90,638	31%
الطاقة والمرافق	16 من 19	23,099 (1,241)	76,227	56%
الإعلام والترفيه	8 من 8	6,016 (51)	10,707	69%
الرعاية الصحية	11 من 11	5,357 (777)	43,262	63%
التأمين	11 من 11	4,624 (80)	9,162	61%
العقارات والإنشاءات	8 من 10	4,229 (97)	21,979	58%
الضيافة والسياحة	8 من 9	3,204 (188)	48,669	85%
التصنيع والصناعة	8 من 9	218 (97)	11,338	64%
الإجمالي	**234 من 250**	**522,128 (30,415)**	**1,856,314**	**30%**

مجاميع الأجهزة حدود دنيا. وتنقسم سجلات بيانات الاعتماد إلى 466,560 سجلاً من قواعد بيانات الاختراقات، و 579,220 سطراً من سجلات برمجيات سرقة المعلومات، و 810,534 مدخلاً من قوائم combolist. وتحتوي الأجهزة المصابة على أكثر من 3.7 مليون من بيانات الاعتماد الملتقطة إجمالاً، لجميع الخدمات وليس لخدمات المؤسسة وحدها.

ما يعنيه ذلك.

- **تقع معظم ارتباطات الأجهزة خارج تصنيف الموظفين.** فمن أصل 522,128 جهازاً، لا يُصنَّف 491,713 جهازاً أجهزةً للموظفين. والأرجح أن كثيراً منها حواسيب المقيمين والعملاء أنفسهم، وإن لم تثبت ملكيتها. وهي إشارة إلى الاحتيال والاستيلاء على الحسابات، ولا تثبت بحد ذاتها وقوع اختراق. أما الأجهزة الـ 30,415 المصنّفة أجهزةً للموظفين فهي المجموعة الفرعية ذات الصلة بالاختراق؛ وتتطلب المجموعتان التحقق.
- **تحمل الجامعات مشكلة أجهزة الموظفين.** فلدى قطاع التعليم 16,760 جهازاً مصنّفاً أجهزةً للموظفين، أي أكثر من نصف الإجمالي الوطني في قائمتنا، و 958,690 سجلاً لبيانات الاعتماد. ويتشارك الموظفون والطلاب النطاقات نفسها، لذا قد تشمل كلمة «الموظفين»

هنا الطلاب.

- **التركّز مرتفع.** ففي قطاع الاتصالات تحمل مؤسستان 94% من سجلات بيانات الاعتماد. لذا فإن مجموع القطاع دليل ضعيف على حال المؤسسة النموذجية.
- **المؤسسة الوسيطة متواضعة.** إذ لدى المؤسسة الوسيطة 274 جهازاً مصاباً و 782 سجلاً لبيانات الاعتماد؛ بينما تحمل أكثر المؤسسات تضرراً عشرات الآلاف.

3.4 الإدراجات الحالية لبيانات الاعتماد

كانت لدى 109 من 250 مؤسسة بيانات اعتماد واحدة على الأقل مرتبطة بنطاقها مُدرجة في سوق مرصودة لبيانات الاعتماد وقت الفحص. ومن بين هذه المؤسسات الـ 109، لدى 99 منها أيضاً سجل إدراجات سابقة.

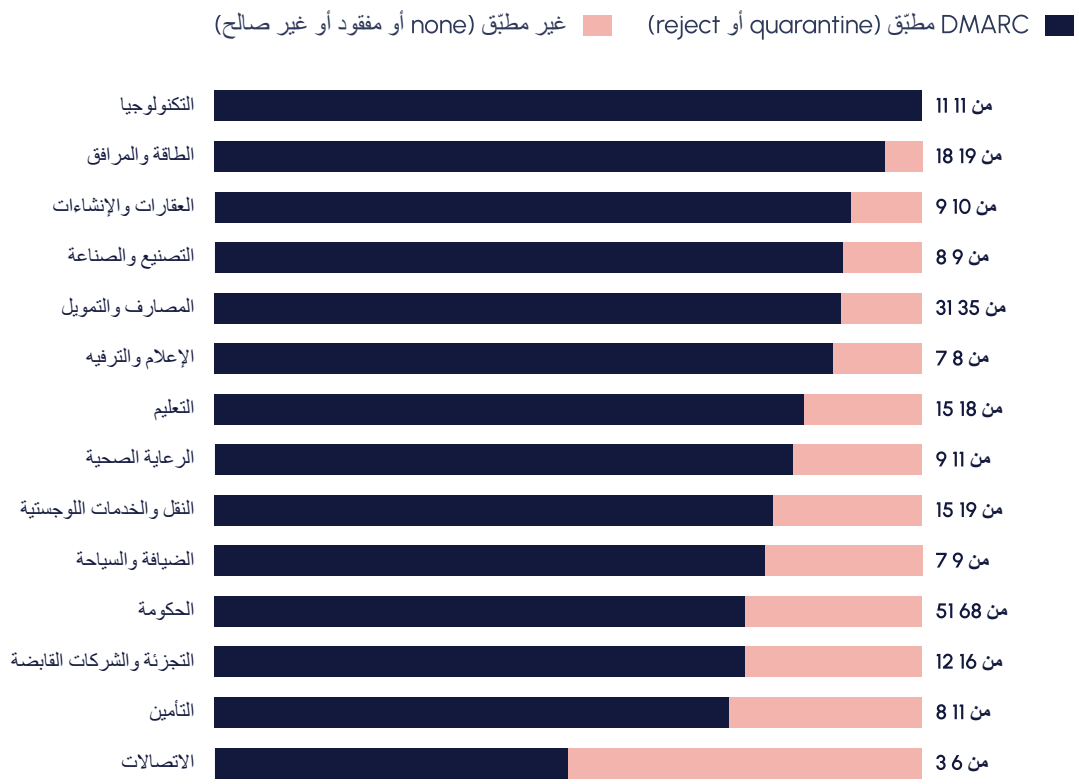
وبالنسبة إلى المدافع، فالإدراج الحالي هو الإشارة السوقية الأكثر مباشرة على أن بيانات دخول مرتبطة بالنطاق معروضة. أما ما إذا كانت تلك البيانات لا تزال صالحة فهو بالضبط ما يجب أن يثبته التحقق. ولا يبيّن الإدراج عدد الحسابات، ولا أصحابها، ولا ما إذا كان الحساب نشطاً، أو محمياً بالمصادقة متعددة العوامل (MFA)، أو أُعيد تعيينه بالفعل. والقرار الذي يدعمه هو «تحقّقوا من الحساب الآن»، لا «أعلنوا وقوع اختراق».

3.5 النطاقات الشبيهة والوثائق المكشوفة والإشارات

- **النطاقات الشبيهة:** كان لدى 205 مؤسسات نطاق شبيه مرشّح واحد على الأقل رُصد حديثاً في آخر 30 يوماً. ولم يُتحقَّق من جميع هذه المطابقات؛ تحقّقوا من كل نطاق قبل التصرّف. النطاقات الشبيهة مرشّحة، وليست مواقع تصيّد احتيالي مؤكدة.
- **الوثائق المكشوفة:** لدى 154 مؤسسة وثيقة مكشوفة واحدة على الأقل تشير إلى نطاقها (3,104 وثائق إجمالاً)، معظمها في القطاع الحكومي.
- **الإشارات:** ذُكرت 89 مؤسسة في مصادر المحادثات المظلمة (قنوات المراسلة) خلال آخر 365 يوماً، و 24 في مصادر الويب المظلم. تقيس أعداد الإشارات الظهور لا العداء؛ إذ تجمع المواقع الإخبارية والبوابات المرتبطة في قنوات Telegram كثيراً منها.

3.6 سلامة البريد الإلكتروني والمواقع

تطبّق معظم القطاعات DMARC؛ ولدى قطاع الاتصالات أكبر حصة من دون تطبيق، ولدى القطاع الحكومي أكبر عدد



المصدر: فحوص Brandefense العامة لـ DNS وTLS والصفحة الرئيسية لـ 250 نطاقاً، 21 نوفمبر 2026 [S4].

نتائج فحوصنا العامة لـ DNS وTLS والصفحات الرئيسية [S4]:

الضابط	النتيجة (من 250 ما لم يُذكر خلاف ذلك)	القراءة
DMARC بسياسة reject	120	يُفترض رفض البريد المنتحل الصادر باسم النطاق
DMARC بسياسة quarantine	84	يُفترض توجيه البريد المنتحل إلى البريد غير المرغوب فيه
DMARC بقيمة p=none أو غير موجود	46 (none 36، و 10 غير موجود)	لا تطبيق؛ انتحال النطاق أسهل
SPF المنتهي بـ -all / ~all / ?all / redirect / none	170 / 69 / 1 / 3 / 7	لا تنشر 7 نطاقات أي سياسة SPF

الضابط	النتيجة (من 250 ما لم يُذكر خلاف ذلك)	القراءة
سجل DKIM موجود	184	عدم العثور عليه لا يثبت غياب DKIM
رصد سجل DS (تفويض DNSSEC)	12	لم يُرصد سجل DS لـ 238 نطاقاً؛ ولا يثبت سجل DS وحده وجود سلسلة ثقة صالحة
شهادة TLS غير صالحة	8 من 222 مفحوصاً	شهادات منتهية الصلاحية أو غير متطابقة أو غير موثوقة
HSTS (HTTP Strict Transport Security) على الصفحة الرئيسية	143 من 173 يمكن الوصول إليها	تفرض معظم المواقع التي يمكن الوصول إليها HTTPS على الزوار العائدين
مزوّد البريد	106 Microsoft 365، و 10 Google، و 8 من دون سجل بريد (MX)	تشغّل البقية بريدها الخاص أو بريداً إقليمياً

السلامة أقوى من الانكشاف. تطبّق 204 من 250 مؤسسة (82%) DMARC، منها 31 من 35 في المصارف والتمويل و 51 من 68 جهة حكومية. ولدى قطاعي الاتصالات (3 من 6 من دون تطبيق) والحكومة (17 من دون تطبيق) أكبر الفجوات (§12.1 الصف 8). وعلى مؤشر السلامة السلبي (الملحق A.5؛ من 0 إلى 100، والأعلى أضعف)، سجّل قطاعا التأمين (38) والاتصالات (36) أضعف قيم مؤشر السلامة بحسب القطاع، وسجّل قطاعا التكنولوجيا (17) والعقارات (19) أقواها. ولا تعوّض سلامة البريد الإلكتروني الجيدة انكشاف بيانات الاعتماد: فالإدراجات الواردة في §3.4 تتعلق ببيانات الدخول لا بالانتحال.

الخلاصات الرئيسية

01

ارتباطات الأجهزة المصابة وبيانات الاعتماد شبه شاملة في القائمة؛ وهي تستدعي التحقق لا الذعر.

02

كانت لدى 109 من 250 مؤسسة إدراجات حالية لبيانات الاعتماد؛ افرزوا هذه الإدراجات أولاً.

03

تطبيق DMARC قوي بنسبة 82%؛ أما تفويض DNSSEC فنادر بواقع 12 من 250.

الفصل 4

ما نرصده على الويب المظلم

يجيب هذا الفصل عن

ماذا ينشر المجرمون عن دولة الإمارات بعد استبعاد رسائل الروبوتات العشوائية، وأي العروض تهمّ فرق الدفاع؟

130,477

منشوراً مصنّفاً على أنه يتعلق بدولة الإمارات، ١ يناير–20 نوفمبر 2026

في هذا الفصل

4.1 بطاقة نطاق البيانات
4.2 المنصات واللغات والحجم
4.3 عائلات الجرائم بعد التنقية
4.4 عروض البيانات الخاصة بالإمارات: بيانات العملاء العقاريين
4.5 العروض ذات الطابع الحكومي والمواد المعاد تداولها
4.6 دراسات حالة
4.7 ما تضيفه المنتديات

باختصار

معظم الحركة السرية المصنّفة على أنها تتعلق بدولة الإمارات إعلانات متعددة البلدان في قنوات Telegram باللغات الإنجليزية والروسية والصينية. بعد التنقية يبقى نحو منشور واحد من كل ثلاثة. ومعظم ما يبقى مخرجات أدوات فحص البطاقات وتجارة الحسابات وتسريبات بيانات متعددة البلدان تذكر الإمارات ضمن بلدان كثيرة. أما العروض الخاصة بالإمارات التي تستحق الاهتمام فهي بيانات عملاء القطاع العقاري، والتحقق من الهوية وبطاقات الإقامة، والوصول إلى أنظمة حكومية على الويب. افحص مصدر كل ادعاء قبل التعليق عليه.

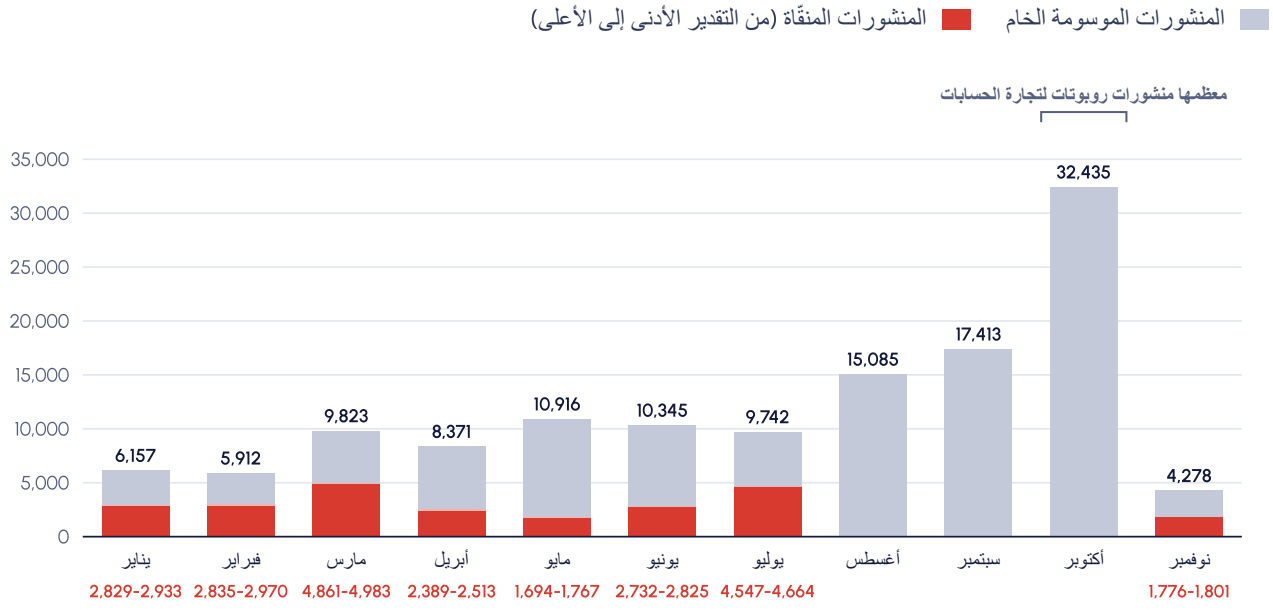
4.1 بطاقة نطاق البيانات

البند	التعريف
المصدر	Brandefense Blackhole: قنوات ومجموعات Telegram، ومجموعة من منتديات الجرائم الإلكترونية، ومواقع اللصق، وDiscord، تُجمع بصورة مستمرة [S1]
تعريف الدولة	وسم دولة («هذا المنشور يتعلق بدولة الإمارات أو يستهدفها أو يذكرها»)، إلى جانب منشورات المنتديات التي تذكر الإمارات

البند	التعريف
الفترة	وقت النشر 1 يناير–20 نوفمبر 2026 (نوفمبر جزئي)
المجموعة الموسومة	130,477 منشوراً محسوباً
التغطية	تغطي نطاقات المنشورات ذات الصلة أشهر يناير–يوليو ونوفمبر (65,544 منشوراً موسوماً)؛ ولا يُغطّى أغسطس وأكتوبر إلا جزئياً، ولم تكن منشورات سبتمبر متاحة
منشورات المنتديات	1,271 منشوراً مميزاً في المنتديات يذكر الإمارات
المنشورات ذات الصلة	تُعرض نطاقاً لأشهر يناير–يوليو ونوفمبر (الملحق A.2)
ما لا يثبته ذلك	أن المنشور الموسوم يستهدف الإمارات، أو أن الادعاء صحيح، أو أن منشورين يتعلقان بالملف نفسه

4.2 المنصات واللغات والحجم

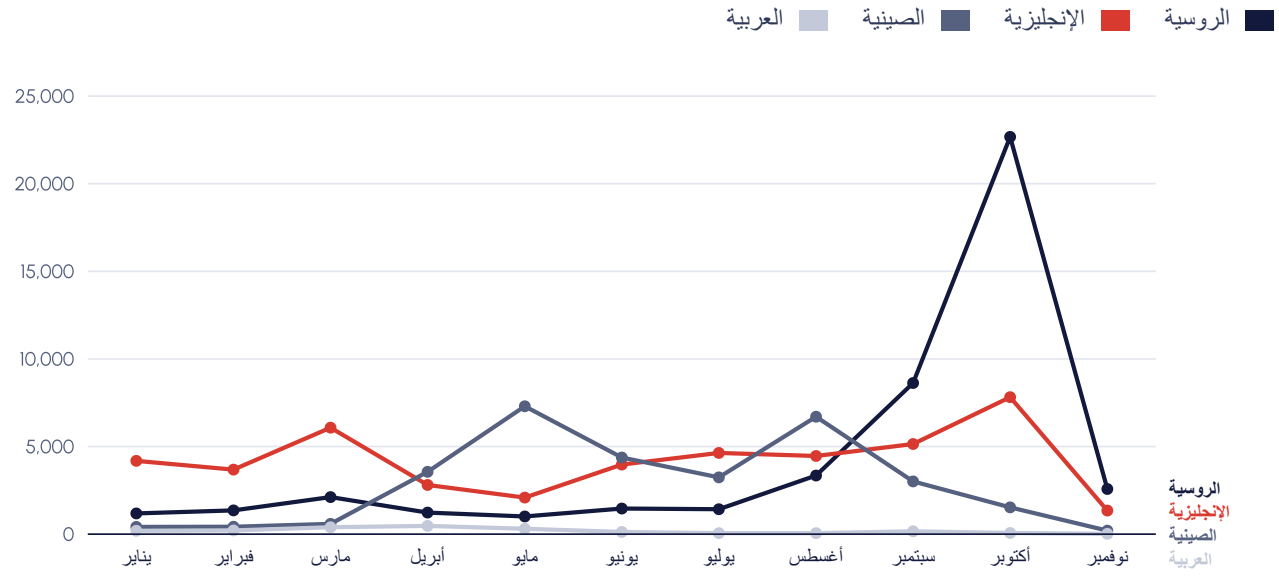
عائلة واحدة من روبوتات تجارة الحسابات تجعل أكتوبر أكبر الأشهر؛ وفي ما عدا ذلك يتراوح الحجم بين نحو 6,000-17,000 منشور موسوم شهرياً



لا يظهر نطاق للمنشورات ذات الصلة من أغسطس إلى أكتوبر لأن التغطية في هذه الأشهر غير مكتملة. المصدر: Brandefense Blackhole، المنشورات الموسومة بأنها تتعلق بالإمارات، تواريخ النشر 1 يناير–20 نوفمبر 2026، ونوفمبر جزئي [S1]. أعداد المنشورات المنقّاة حدّ أعلى.

المقياس	القيمة
حصة Telegram من المنشورات الموسومة	99.64% (130,007)
منشورات المنتديات	381 منشوراً موسوماً، إضافة إلى 1,271 منشوراً مميزاً في المنتديات يذكر الإمارات
مواقع اللصق وDiscord	39، 50
الروسية / الإنجليزية / الصينية / العربية	36.0% / 35.4% / 24.0% / 1.6% من المنشورات الموسومة (قد يحمل المنشور الواحد أكثر من لغة)
أكبر الأشهر	أكتوبر، 32,435 منشوراً، منها 19,924 منشوراً لتجارة الحسابات

الروسية والإنجليزية تهيمنان على وسم الإمارات؛ والعربية أقل من 2% من المنشورات



يحمل Telegram نسبة 99.64% من المنشورات الموسومة. قد تتداخل تصنيفات اللغة. المصدر: Brandefense Blackhole، المنشورات الموسومة بأنها تتعلق بالإمارات، تواريخ النشر 1 يناير–20 نوفمبر 2026، ونوفمبر جزئي [S1]. أعداد المنشورات المنقّاة حدّ أعلى.

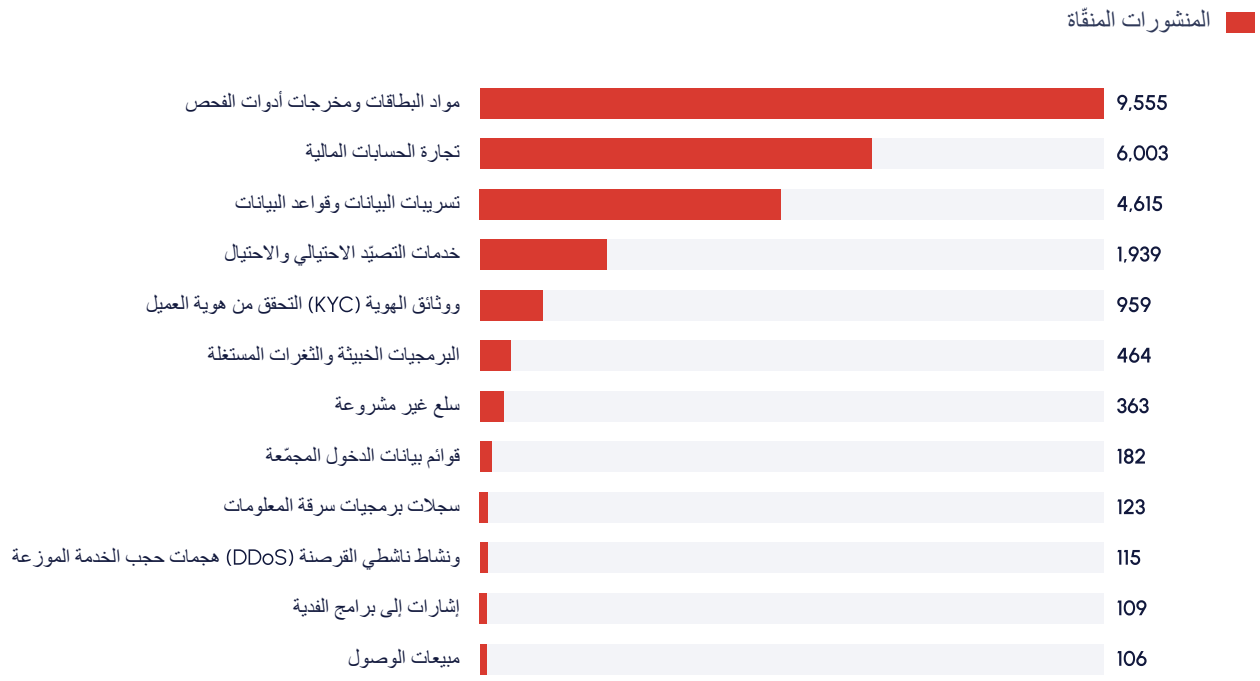
أكتوبر شهر روبوتات، لا شهر هجمات. كانت 61% من منشورات أكتوبر الموسومة منشورات لتجارة الحسابات، وهيمنت عليها قوالب قوائم أسعار مكررة. وبالطريقة نفسها ضخّمت الإعلانات باللغة الصينية أرقام الفترة من أبريل إلى أغسطس. وتُظهر المملكة العربية السعودية ارتفاعاً أكبر في يناير–فبراير (729,186 منشوراً في شهرين)، وتُظهر قطر ارتفاعاً في أكتوبر (42,835). لذلك تدل هذه الارتفاعات على حملات الروبوتات أكثر مما تدل على بلد بعينه.

العربية نادرة في الفضاء السري الخاص بالإمارات الذي نرصده. 2,070 منشوراً موسوماً فقط (1.6%) باللغة العربية. وتجري التجارة الإجرامية المتعلقة بالإمارات في الغالب بالإنجليزية والروسية، وتستهدف سكاناً مقيمين متعددي اللغات أصلاً (§2.1).

4.3 عائلات الجرائم بعد التنقية

في الفترة يناير–يوليو ونوفمبر، يبلغ عدد المنشورات ذات الصلة (بعد التنقية) 23,663–24,456 من أصل 65,544 منشوراً موسوماً (36.1–37.3%)، وتُعرض نطاقاً. ومن بين 30 منشوراً عشوائياً ذا صلة، كان 27 منها متعلقاً بالجريمة، لكن 10 فقط ذكرت الإمارات تحديداً. لذلك تمثل الأعداد بعد التنقية حداً أعلى للنشاط الإجرامي الخاص بالإمارات.

مخرجات فحص البطاقات وتجارة الحسابات تهيمن على المنشورات المنقّاة؛ ومبيعات الوصول نادرة



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

العائلة (منشورات منقّاة، يناير–يوليو ونوفمبر)	المنشورات	ما يغلب عليها
مواد البطاقات ومخرجات أدوات الفحص	9,555	مخرجات روبوتات تختبر بطاقات، صدر كثير منها عن بنوك إماراتية (§8.2)
تجارة الحسابات المالية	6,003	حسابات بنكية ومحافظ وحسابات منصات تداول؛ تجنيد حسابات وسيطة لتمرير الأموال (mule)

العائلة (منشورات منقّاة، يناير–يوليو ونوفمبر)	المنشورات	ما يغلب عليها
تسريبات البيانات وقواعد البيانات	4,615	قوائم عملاء محتملين متعددة البلدان؛ وأقلية من مجموعات بيانات خاصة بالإمارات
خدمات التصيّد الاحتيالي والاحتيال	1,939	إساءة استخدام روابط الدفع، وأدوات الاحتيال، وتجنيد من يُسمَّون «shooter»
التحقق من هوية العميل (KYC) ووثائق الهوية	959	خدمات التحقق من بطاقات الإقامة وجوازات السفر
البرمجيات الخبيثة والثغرات المستغلة	464	بيع أدوات؛ والقليل منها خاص بالإمارات
قوائم بيانات الدخول المجمّعة وسجلات برمجيات سرقة المعلومات	305	أسطر بيانات اعتماد لبنوك وبوابات وشركات طيران إماراتية
هجمات حجب الخدمة الموزعة (DDoS) ونشاط ناشطي القرصنة	115	ادعاءات في مارس ضد مواقع اتحادية (الفصل 6)
مبيعات الوصول	106	وصول إلى أنظمة ويب حكومية ومؤسسية (§4.5)
عائلات أخرى	472	سلع غير مشروعة (363) وإشارات إلى برامج الفدية (109)

لا نقارن أعداد العائلات عبر يونيو 2026. وقد ينتمي المنشور الواحد إلى أكثر من عائلة.

4.4 عروض البيانات الخاصة بالإمارات: بيانات العملاء العقاريين

كانت البيانات العقارية أكثر فئات البيانات الخاصة بالإمارات عرضاً في المنشورات التي راجعناها. على مدار العام أدرج تسعة بائعين على الأقل بيانات عن ملّاك عقارات ومستأجرين ومستخدمي بوابات. وتراوحت الادعاءات بين قائمة ملّاك من 74,000 سطر لمجمّع سكني واحد و 986,506 سجلات حسابات من خدمة عقارية إماراتية تتضمن حقولاً مرتبطة بكلمات المرور. وكانت الأسعار المطلوبة منخفضة، حتى 1,200 USD، ونُشرت مجموعة واحدة مجاناً. وفي فبراير طلب مشترٍ قاعدة بيانات وكالة عقارية بملايين الأسطر، قبل موجة الإدراجات في أبريل–مايو.

التاريخ	العرض (بحسب الادعاء)	السعر	البطاقة
2026-02-18	مشترٍ يبحث عن نظام إدارة علاقات العملاء (CRM) لوكالة في دبي بملايين الأسطر	غير متاح	B20

التاريخ	العرض (بحسب الادعاء)	السعر	البطاقة
2026-04-02	بيانات عملاء ومبيعات ووثائق هوية لمطوّر عقاري في دبي	USD 100	B02
2026-04-13	400,000 سجل ملّاك ومستأجرين منسوبة إلى مطوّر كبير، رُفعت إلى 700,000 بعد ستة أيام	غير مذكور	B04
2026-05-06	986,506 سجلات حسابات من خدمة عقارية إماراتية	مجاناً	B06
2026-09-10	قاعدة بيانات منصة عقارية بحجم 49GB، مع ادعاء بمسحها بعد ذلك	غير مذكور	B05

أصرّ أحد البائعين على أن مجموعته ليست «البيانات العامة» لملّاك دبي التي قال إن «الجميع» يبيعها، وهذا إقرار بأن مثل هذه القوائم متداولة أصلاً. يُضعف ذلك تفرّد كل ادعاء، لكنه لا يُضعف الخطر. فتفاصيل الملّاك والمستأجرين والمعاملات هي بالضبط ما يحتاجه الاحتيال القائم على تعليمات الدفع والتسليم الوهمي للعقار.

بطاقة الدليل B20 — 18 فبراير 2026

مشترٍ مجهول منتدى تسريبات · Forum · الإنجليزية

النص الأصلي

I am looking for a big Realty Estate Agency database from United Arab Emirates (Dubai if i'm not wrong) with couple millions lines also in thread title was just domain name and description was said that base from CRM. I lost link to thread

الترجمة

أبحث عن قاعدة بيانات كبيرة لوكالة عقارات من الإمارات العربية المتحدة (دبي إن لم أكن مخطئاً) تضم بضعة ملايين من الأسطر، وكان عنوان سلسلة النقاش مجرد اسم نطاق، وذُكر في الوصف أن القاعدة من نظام CRM. فقدت رابط سلسلة النقاش

ملاحظة. سبق الطلب على البيانات العقارية موجة إدراجات شركات التطوير والبوابات العقارية في أبريل ومايو.

ما يمكن إثباته — بحث مشترٍ عن قاعدة بيانات CRM لوكالة عقارات في دبي تضم ملايين الأسطر، شوهدت سابقاً في المنتدى.

ما لم يثبت — لا يثبت ذلك وجود قاعدة بيانات كهذه.

بطاقة الدليل B04 — 13 أبريل 2026

ksa901 منتدى تسريبات · Forum · الإنجليزية

النص الأصلي

I am selling here [major Dubai property developer] - owners & rentals information, Datasets have more than 400k records of owners and rentals and even they car information and even their parking and address, phone numbers, emails. and included 4gb of Docs. [...] is not public Data of Dubai owners which everyone sell

الترجمة

أبيع هنا [شركة تطوير عقاري كبرى في دبي] - بيانات الملاك والمستأجرين، تضم مجموعات البيانات أكثر من 400 ألف سجل للملاك والمستأجرين، وحتى بيانات سياراتهم ومواقف سياراتهم وعناوينهم وأرقام هواتفهم وبريدهم الإلكتروني. وتشمل 4gb من المستندات. [...] ليست بيانات عامة لملاك دبي التي يبيعها الجميع

ملاحظة. بعد ستة أيام رفع الاسم المستعار نفسه ادعاءه إلى 700,000 سجل تشمل شركة تطوير ثانية.

ما يمكن إثباته — أعلن بائع عن 400,000 سجل لملاك ومستأجرين، مع تفاصيل السيارات ومواقفها، منسوبة إلى شركة تطوير عقاري كبرى في دبي.

ما لم يثبت — لا يثبت ذلك النظام المصدر، وصياغة البائع نفسه تقرّ بأن قوائم مشابهة لملاك دبي متداولة أصلاً.

بطاقة الدليل B02 — 2 أبريل 2026

بائع البطاقة B01 (الاسم المستعار محجوب) منتدى تسريبات · Forum · الإنجليزية

النص الأصلي

```
[Dubai real-estate developer] is Real estate company in dubai [...] Price: 100$ [...] I got customers Info / sales info / id,passport pics + bank transactions / CRM
```

الترجمة

[شركة تطوير عقاري في دبي] شركة عقارات في دبي [...] السعر: 100$ [...] لديّ بيانات العملاء / بيانات المبيعات / صور الهويات وجوازات السفر + المعاملات المصرفية / CRM

ملاحظة. عرض اسم مستعار ثانٍ مجموعة أعمدة CRM نفسها في منتدى آخر في 19 أبريل، مدّعياً الحصول على 350GB من حساب مدير مبيعات.

ما يمكن إثباته	عرضت المجموعة نفسها من الحسابات المرتبطة بالجهة الفاعلة بيانات عملاء ومبيعات ووثائق هوية لشركة تطوير عقاري في دبي مقابل 100 دولار.
ما لم يثبت	لا يثبت ذلك حجم السجلات، ولا أن صور جوازات السفر حقيقية.

بطاقة الدليل B06 — 6 مايو 2026

attackercompany منتدى تسريبات · Forum · الإنجليزية

النص الأصلي

```
UAE REAL ESTATE DATA REPORT [...] Total Records: 986,506 Region: United Arab Emirates Sector: Real Estate [...] Fields Observed • Name • Login Identifiers • Password-Related Values • Phone / Cell Numbers • Email Addresses • WhatsApp Information • IP Addresses
```

الترجمة

تقرير بيانات العقارات في الإمارات [...] إجمالي السجلات: 986,506 المنطقة: الإمارات العربية المتحدة القطاع: العقارات [...] الحقول المرصودة · الاسم · معرّفات تسجيل الدخول · قيم متعلقة بكلمات المرور · أرقام الهاتف / الجوال · عناوين البريد الإلكتروني · معلومات واتساب · عناوين IP

ملاحظة. جزء من مجموعة امتدت على مدار العام تضم تسع مجموعات بيانات على الأقل لملاك العقارات والقطاع العقاري.

ما يمكن إثباته	أعلن منشور عن مجموعة بيانات مزعومة تضم 986,506 سجلاً من خدمة عقارية إماراتية، مع حقول مرتبطة بكلمات المرور وبيانات الاتصال.
ما لم يثبت	لا يثبت ذلك المنصة التي جاءت منها السجلات. وقد سمّت إعادة نشر لاحقة بوابة عقارية إماراتية دون دليل.

4.5 العروض ذات الطابع الحكومي والمواد المعاد تداولها

كانت العروض ذات الطابع الحكومي في 2026 في معظمها نقاط دخول وملفات معاد تداولها، لا مجموعات بيانات وطنية جديدة.

- **إعادة التداول.** أُعيد نشر مجموعة بيانات طلابية، يؤرخها ناشروها إلى مارس 2025، في خمسة منتديات على الأقل من يناير إلى مايو (B07).
- **الوصول.** عُرض في أبريل وصول بصلاحيات مدير أعلى إلى نظام ويب لدائرة مالية في إحدى الإمارات مقابل 800 (B08) USD.
- **الاستطلاع.** رسمت حزمة في مارس خريطة للأنظمة الخلفية لخدمة ذكاء اصطناعي تابعة لدائرة حكومية، ولبوابة PHP منتهية الدعم (B09).

- **قوائم السكان**. أعلنت جهة فاعلة واحدة عن 30,000 سجل لأفراد شرطة في فبراير، ثم عن 180,000 سجل لمقيمين أجانب من جنسية واحدة بعد أسبوعين (B10).
- **أسطر بيانات الاعتماد**. حملت عمليات رفع آلية للسجلات أسطر بيانات اعتماد لصفحة تسجيل دخول إلى خدمات إلكترونية حكومية (B12).
- **قوائم الانكشاف**. نُشرت في 5 مارس قائمة مجانية بنحو 185,000 بث لكاميرات مكشوفة على الإنترنت في الإمارات (B11).

بطاقة الدليل B07 — 26 يناير 2026

Retrogade منتدى تسريبات · Forum · الإنجليزية

النص الأصلي

```
In March 2025, [an education
organisation] experienced a
significant data breach. The
compromised dataset includes [...]
This breach primarily affects
students
```

الترجمة

في مارس 2025، تعرّضت [مؤسسة تعليمية] لاختراق بيانات كبير. تتضمن مجموعة البيانات المخترقة [...] ويطال هذا الاختراق الطلاب بشكل أساسي

ملاحظة. أُعيد نشرها في خمسة منتديات على الأقل بين يناير ومايو. وأُفيد في عدة سلاسل نقاش بأن روابط التنزيل معطلة.

ما يمكن إثباته	أُعيد نشر مجموعة بيانات طلابية منسوبة إلى مؤسسة تعليمية للتنزيل المجاني في يناير 2026.
ما لم يثبت	لا يثبت ذلك وقوع حادثة جديدة في 2026، إذ يؤرخ المنشور الادعاء الأصلي إلى مارس 2025.

بطاقة الدليل B08 — 26 أبريل 2026

Crimson منتدى تسريبات · Forum · الإنجليزية

النص الأصلي

```
Today I'm selling UAE [an emirate's
finance department] Super
Administrator Access. Proof: [link
removed] Price: 800 USD Contact
(session only): [contact removed]
```

الترجمة

اليوم أبيع وصول المسؤول الأعلى (Super Administrator) إلى [الدائرة المالية في إحدى الإمارات] في الإمارات. الدليل: [تمت إزالة الرابط] السعر: 800 USD للتواصل (عبر Session فقط): [تمت إزالة جهة الاتصال]

ملاحظة. أقل عروض الوصول إلى جهات حكومية سعراً في مجموعة البيانات المرصودة.

ما يمكن إثباته	عرض بائع وصول المسؤول الأعلى إلى نظام ويب تابع للدائرة المالية في إحدى الإمارات مقابل 800 دولار.
ما لم يثبت	لا يثبت ذلك التطبيق الذي يشمله الوصول، ولا ما إذا كان لا يزال صالحاً.

بطاقة الدليل B09 — 23 مارس 2026

rSosa منتدى تسريبات · Forum · الإنجليزية

النص الأصلي

```
I've spent the last week mapping [an
emirate government department] [...]
AI BRAIN: [exposed LLM-orchestration
back-ends]. These are the backends
for [a government AI service] [...]
THE HOLE: [an end-of-life PHP portal]
[...] ADMIN ACCESS: [portal instances
with authentication
misconfigurations].
```

الترجمة

أمضيت الأسبوع الماضي في رسم خريطة [دائرة حكومية في إحدى الإمارات] [...] العقل الذكي (AI BRAIN): [واجهات خلفية مكشوفة لتنسيق النماذج اللغوية الكبيرة]. هذه هي الأنظمة الخلفية لـ [خدمة حكومية بالذكاء الاصطناعي] [...] الثغرة (THE HOLE): [بوابة PHP منتهية الدعم] [...] وصول المسؤول: [نسخ بوابات فيها أخطاء في إعدادات المصادقة].

ملاحظة. مثال مبكر على بيع استطلاع منصات الذكاء الاصطناعي ضد خدمة حكومية بالذكاء الاصطناعي.

ما يمكن إثباته

عرض بائع حزمة استطلاع لمنظومة الذكاء الاصطناعي والويب لدى دائرة حكومية. وتسمّي الحزمة نقاط نهاية مكشوفة لتنسيق النماذج اللغوية الكبيرة (LLM) وبوابة PHP منتهية الدعم.

ما لم يثبت

لا يثبت ذلك أن البائع تمكّن من الدخول أو أخذ أي بيانات.

بطاقة الدليل B12 — 11 أغسطس 2026

روبوت X Forum منتدى لتجميع التسريبات · Forum · الإنجليزية

النص الأصلي

```
[a government e-services portal]
Uploaded by X FORUMS [...] Content
Type: URL / Email / Password Combo
```

الترجمة

[بوابة خدمات إلكترونية حكومية] رفعها X FORUMS [...] نوع المحتوى: رابط / بريد إلكتروني / كلمة مرور (Combo)

ملاحظة. نشر الحساب الآلي نفسه مقتطفات سجلات لمصرف تجزئة إماراتي، وشركة طيران إماراتية، ومواقع تجارة إلكترونية فاخرة.

ما يمكن إثباته

ظهرت أسطر بيانات اعتماد لصفحة تسجيل دخول إلى خدمات إلكترونية حكومية ضمن رفع آلي لسجلات.

ما لم يثبت

لا يثبت ذلك أن الحسابات كانت صالحة، ولا حدوث خرق للبوابة نفسها. فهذه الأسطر تأتي عادةً من أجهزة مستخدمين مصابة.

بطاقة الدليل B10 — 24 فبراير 2026

TheAshborn منتدى تسريبات · Forum · الإنجليزية

النص الأصلي

```
30,000 Police Personnel
Information(PII) (Full Details) from
United Arab Emirates Screenshot as
proof: [link removed] for more proof
just contact us No Telegram - No TOX
- Just Session
```

الترجمة

بيانات شخصية (PII) لـ 30,000 من أفراد الشرطة (تفاصيل كاملة) من الإمارات العربية المتحدة لقطة شاشة كدليل: [تمت إزالة الرابط] لمزيد من الأدلة تواصلوا معنا فقط لا Telegram - لا TOX - فقط Session

ملاحظة. بعد أسبوعين أدرج الاسم المستعار نفسه 180,000 سجل لمقيمين أجانب من جنسية واحدة، بالتنسيق نفسه ومع التواصل عبر Session فقط.

ما يمكن إثباته — أعلنت جهة فاعلة عن بيانات شخصية لـ 30,000 من أفراد الشرطة في الإمارات، ولم تقدّم دليلاً سوى لقطة شاشة.

ما لم يثبت — لا يثبت ذلك مصدر البيانات ولا اكتمالها ولا دقتها.

بطاقة الدليل B11 — 5 مارس 2026

CVDEAD منتدى تسريبات · Forum · الإنجليزية

النص الأصلي

```
I'm sharing this dataset, which
contains a curated list of publicly
accessible IoT devices within the
United Arab Emirates (UAE)
infrastructure that expose their
video streams via RTSP
(protected/unprotected) [...] UAE IoT
| Vuls Server:Port | RTSP CAM | 185K
```

الترجمة

أشارك مجموعة البيانات هذه، التي تحتوي على قائمة منتقاة من أجهزة إنترنت الأشياء المتاحة للعموم ضمن البنية التحتية للإمارات العربية المتحدة (UAE) والتي تكشف بث الفيديو الخاص بها عبر RTSP (محمي/غير محمي) [...] UAE IoT | Vuls Server:Port | RTSP CAM | 185K

ملاحظة. شوركت في 5 مارس. وهي ذات صلة بانكشاف كاميرات الأمن المادي.

ما يمكن إثباته — شوركت مجاناً قائمة تضم نحو 185,000 نقطة نهاية لبث كاميرات مكشوفة على الإنترنت في الإمارات، أُعدّت عبر المسح، خلال ما وصفه المجلس بفترة التصعيد.

ما لم يثبت — لا يثبت ذلك الوصول إلى أي بث دون تصريح.

4.6 دراسات حالة

تعرض كل حالة الادعاء وما يمكننا إثباته واستجابة متناسبة، مع التسلسل الزمني والبدائل والحدود حيث تسمح الأدلة بذلك. واستجابات الحالات نقاط بداية؛ أما الإجراءات المُسندة، مع الجهات المسؤولة وأدلة الإنجاز، فهي في §12.1.

A

الحالة A

ملف عملاء شركة تأمين نُشر على تيليغرام وفي ثلاثة منتديات

ادعاء غير مؤكد

بطاقة الدليل B01 | 30 يناير 2026 | منتدى تسريبات | التأمين

الادعاء	أعلن بائع عن نحو 80,000 سجل لعملاء ووسطاء منسوبة إلى شركة تأمين إماراتية مقابل 200 USD، وقال إنها مصفّاة من 500,000 صف. وتشمل الحقول المدرجة أرقام الهوية الوطنية وبيانات الاتصال والمبالغ المدفوعة.
التسلسل الزمني	إعلان تشويقي على Telegram في 28 يناير؛ ثم الإدراج الكامل في 30 يناير؛ ثم إعادة إدراج في منتديين آخرين في 2 و 25 أبريل بالاسم المستعار نفسه.
ما يمكننا إثباته	أن اسماً مستعاراً واحداً أبقى الإدراج نفسه الخاص بالمؤسسة قائماً ثلاثة أشهر. وكتب البائع أن الوصول فُقد مبكراً، وهذا يتوافق مع تسجيل دخول قصير الأمد لا مع وصول مستمر.
البدائل	بيانات مصدرها وسيط، أو مورّد خارجي لنظام إدارة علاقات العملاء، أو جهة تجميع بيانات؛ أو سجلات قديمة معاد تدويرها.
الحدود	لم نحصل على العينة. ولم تعلّق شركة التأمين ولا أي جهة رسمية حتى تاريخ الإقفال لدينا.
الاستجابة	ينبغي لشركات التأمين والوسطاء مراجعة سجلات الوصول إلى أنظمة إدارة علاقات العملاء وبوابات الدفع لشهر يناير 2026، وتدوير بيانات اعتماد التكامل، والاستعداد لرسائل تصيّد احتيالي تقتبس تفاصيل الوثائق (§12.1 الصفان 14-15).

الخلاصة

استعدّوا لاحتمال إساءة استخدام الحقول المُعلن عنها، وراجعوا وصول نظام CRM والوسطاء قبل أن يتحدث أحد عن اختراق.

B

الحالة B

إدراجان يذكران هيئة النقل في إحدى الإمارات

بطاقة الدليل B03 | 15 نوفمبر 2026 | منتدى تسريبات

الحكومة، النقل

ادعاء غير مؤكد

الادعاء	في 25 أبريل عرض بائع 301 ملف من التصاريح والمخططات والبريد الإلكتروني مقابل 800 USD. وفي 15 نوفمبر أدرج بائع آخر «اختراق قاعدة بيانات» بحجم 50GB مقابل 5,000 USD، مدعياً أنها تضم 450,000 سجل خدمات للمقيمين و 100,000 سجل للسائقين مع حقول الهوية وجواز السفر والتأشيرة.
ما يمكننا إثباته	أن اسمين مستعارين لا صلة بينهما ذكرا الجهة الحكومية نفسها بفارق سبعة أشهر، ووصفا بيانات مختلفة: وثائق مشاريع أولاً، ثم مجموعة بيانات عملاء مرتبطة بالهوية. ولم تُنشر أي عينة في المنشورات التي قرأناها.
البدائل	صناديق بريد مقاولين أو استشاريين بالنسبة لملفات أبريل؛ وبالنسبة لنوفمبر، قائمة حقول مبنية من مصادر أخرى مرتبطة بالهوية، أو مختلقة لرفع السعر.
الحدود	لم يتناول أي بيان رسمي أياً من الإدراجين حتى تاريخ الإقفال لدينا.
الاستجابة	ينبغي للهيئة ومقاوليها مراجعة انكشاف أنظمة إدارة الوثائق والبريد الإلكتروني منذ الربع الثاني. وينبغي تحذير المقيمين من انتحال الصفة باستخدام تفاصيل الرخص والتأشيرات إذا جرى التحقق من عينة (§12.1 الصفان 4 و 15).

الخلاصة

سمّى بائعان لا صلة بينهما الجهة نفسها؛ تحققوا من أي عينة قبل التعليق، وجهّزوا تحذيرات للمقيمين.

بطاقة الدليل B01 — 30 يناير 2026

بائع بيانات شركة التأمين (الاسم المستعار محجوب)

منتدى تسريبات · Forum · الإنجليزية

النص الأصلي

```
Welcome To Another UAE Data breach
[UAE insurer] (80k record) [...]
Price: 200$ [...] CRM (Payments
invoice, customers info, brokers
info) UAE Id card, full name, email,
phone number, address, paid amount
[...] the total was 500k record i
filtered so i got 80k [...] i lost
the access early
```

الترجمة

مرحباً بكم في اختراق بيانات إماراتي آخر [شركة تأمين إماراتية] (80 ألف سجل) [...] السعر: 200$ [...] نظام CRM (فواتير المدفوعات، بيانات العملاء، بيانات الوسطاء) بطاقة الهوية الإماراتية، الاسم الكامل، البريد الإلكتروني، رقم الهاتف، العنوان، المبلغ المدفوع [...] كان الإجمالي 500 ألف سجل، قمت بتصفيتها فحصلت على 80 ألفاً [...] فقدت الوصول مبكراً

ملاحظة. نُشر الإدراج نفسه على تيليغرام وفي ثلاثة منتديات بين يناير وأبريل. ويربط الاسم المستعار الإدراج بحساب على تيليغرام أعلن أيضاً عن مجموعة بيانات لشركة تطوير عقاري في دبي.

ما يمكن إثباته

أعلن بائع عن مستخرج من نظام CRM يضم 80,000 سجل لعملاء ووسطاء، منسوب إلى شركة تأمين إماراتية، مقابل 200 دولار، وأدرج أرقام الهوية الوطنية ضمن الحقول.

ما لم يثبت

لا يثبت ذلك أن البيانات مصدرها أنظمة شركة التأمين، ولا أن أي عملية بيع قد تمت.

بطاقة الدليل B03 — 15 نوفمبر 2026

databreach000

منتدى تسريبات · Forum · الإنجليزية

النص الأصلي

```
[an emirate's transport authority]
Database Breach __50GB [...] Price :
$5K Exposed Services and Records : 1.
Citizen and Resident Service (450K
Unique Records) [...] 2. Drivers
Service (100K unique Records + 35K
Driver License PDF)
```

الترجمة

[هيئة النقل في إحدى الإمارات] اختراق قاعدة بيانات __50GB [...] السعر: 5K$ الخدمات والسجلات المكشوفة: 1. خدمة المواطنين والمقيمين (450 ألف سجل فريد) [...] 2. خدمة السائقين (100 ألف سجل فريد + 35 ألف ملف PDF لرخص القيادة)

ملاحظة. ظهر إدراج سابق أصغر (301 ملف، 800 دولار) للهيئة نفسها في منتدى آخر في 25 أبريل باسم مستعار مختلف.

ما يمكن إثباته

أدرج بائع مجموعة بيانات بحجم 50GB منسوبة إلى هيئة النقل في إحدى الإمارات مقابل 5,000 دولار، مع قائمة حقول تشمل أرقام الهوية وجواز السفر والتأشيرة.

ما لم يثبت

لا يثبت ذلك الوصول إلى أنظمة الهيئة، إذ يمكن تجميع قائمة الحقول من مصادر أخرى.

C

الحالة C

البيانات العقارية بوصفها سوقاً (B04, B06)

سوق مرصودة

العقارات

الادعاء	أدرج تسعة بائعين على الأقل بيانات ملّاك ومستأجرين ومطوّرين وبوابات خلال العام (§4.4).
ما يمكننا إثباته	أن القطاع العقاري أنتج إدراجات خاصة بالإمارات على مستوى المؤسسات وعلى مستوى السكان أكثر من أي قطاع آخر في بياناتنا. وسبقت منشوراتُ الطلب موجةَ العرض.
البدائل	يُرجَّح أن كثيراً من هذه المجموعات أُعيد بناؤه من قوائم الوسطاء والبوابات المكشوطة ومستخرجات أقدم متداولة أصلاً.
الحدود	تتداخل قوائم الملّاك بدرجة كبيرة؛ وأعداد السجلات مدّعاة وغير مُتحقق منها.
الاستجابة	ينبغي للمطوّرين والوسطاء والبوابات مراجعة صادرات أنظمة إدارة علاقات العملاء ووصول الشركاء، وتحذير الملّاك من الاحتيال القائم على تعليمات الدفع والتسليم الوهمي (§12.1، الصفان 14-15).

الخلاصة

بيانات الملاك والمستأجرين متداولة على نطاق واسع؛ احموا الملاك من الاحتيال في تعليمات الدفع وتسليم العقارات.

D

الحالة D

مجموعة بيانات طلابية من 2025 يُعاد تداولها

بيانات أُعيد تداولها

بطاقة الدليل B07 | 26 يناير 2026 | منتدى تسريبات

التعليم

الادعاء	أُعيد نشر مجموعة بيانات طلابية تتضمن أرقام هوية وبيانات اتصال ودرجات وتفاصيل مدارس، منسوبة إلى مؤسسة تعليمية، للتنزيل المجاني.
ما يمكننا إثباته	يصفها كل ناشر بأنها الحدث نفسه الذي وقع في مارس 2025؛ وتشير عدة سلاسل نقاش إلى روابط معطّلة. ولا شيء في بياناتنا يشير إلى عملية تسلل جديدة في 2026.
البدائل	مورّد لنظام إدارة مدرسية، أو منصة واحدة، بوصفه المصدر الأصلي.
الاستجابة	ينبغي للمدارس توقّع رسائل تصيّد احتيالي موجهة إلى الطلاب وأولياء الأمور تقتبس تفاصيل المدرسة والدرجات، والتحقق مما إذا كانت أي حقول لبيانات الاعتماد لا تزال صالحة (§12.1، الصفان 2 و 15).

الخلاصة

ادعاء يعود إلى 2025 لا يزال متداولاً؛ توقعوا تصيّداً احتيالياً بموضوعات مدرسية، وأعيدوا تعيين أي بيانات اعتماد مُعاد استخدامها.

E

الحالة E

عروض وصول واستطلاع تستهدف جهات حكومية في الإمارات المحلية (B08, B09)

الحكومة

عرض غير مؤكد

الادعاء	وصول بصلاحيات مدير أعلى إلى نظام ويب لدائرة مالية (USD 800، أبريل)، وحزمة استطلاع عن منظومة الذكاء الاصطناعي والويب لدائرة حكومية (مارس).
ما يمكننا إثباته	عرض بائعون مختلفون نقاط دخول إلى أنظمة حكومية للويب والذكاء الاصطناعي، لا مجموعات بيانات جاهزة. وحزمة مارس هي أوضح مثال في بياناتنا على استطلاع منصات ذكاء اصطناعي معروض للبيع.
البدائل	وصول إلى تطبيق فرعي محدود القيمة؛ أو استطلاع مبني على المسح العلني وحده.
الحدود	لم تتوفر لدينا لقطات شاشة تثبت ذلك؛ والصلاحية والنطاق غير معروفين.
الاستجابة	ينبغي للجهات الحكومية حصر نقاط تنسيق الذكاء الاصطناعي المكشوفة على الإنترنت والبوابات منتهية الدعم، وفرض تسجيل الدخول الموحّد على منصات إدارة المحتوى، وإزالة حسابات المدير المحلية (§12.1 الصف 4).
الخلاصة	**المعروض للبيع كان نقاط دخول لا مجموعات بيانات؛ اجردوا واجهات الإدارة ونقاط نهاية الذكاء الاصطناعي المكشوفة على الإنترنت.**

F

الحالة F

حادثة مؤكدة في برنامج ولاء لقطاع التجزئة وإدراج في موقع تسريب في الأسبوع نفسه

التجزئة

حادثة أكدتها الشركة

الادعاء	في 10 نوفمبر أدرجت مجموعة تدير موقع تسريب لبرامج الفدية Landmark Group، مجموعة التجزئة التي تتخذ من دبي مقراً لها، بحسب Ransompedia [S5].
الرواية الرسمية	في 11 نوفمبر قالت Landmark Group إنها رصدت وصولاً غير مصرح به إلى أحد أنظمتها أثّر على أعضاء برنامج الولاء Shukran. وقالت إن الأسماء وبيانات الاتصال وتواريخ الميلاد ربما كُشفت، وإن بيانات البطاقات لم تتأثر، وإن الجهات التنظيمية وجهات إنفاذ القانون أُبلغت [S24][S25].
ما يمكننا إثباته	حادثة مؤكدة لدى الشركة، وادعاء في موقع تسريب ضدها، في غضون يوم واحد. ولم تذكر الشركة أي مجموعة لبرامج الفدية، لذلك لم نثبت أن الأمرين يشيران إلى الحدث نفسه.
الاستجابة	ينبغي لأعضاء برنامج الولاء توقّع رسائل تصيّد احتيالي تقتبس أسماءهم وتواريخ ميلادهم. وينبغي لتجار التجزئة الذين يشغّلون منصات ولاء أن يعاملوها بوصفها أنظمة هوية: مراقبة عمليات التصدير، وحماية وصول المديرين بالمصادقة متعددة العوامل، وإعداد إشعارات الأعضاء مسبقاً (§12.1، الصفان 14-15).
الخلاصة	**حادثة مؤكدة في منصة برنامج الولاء؛ ربما كُشفت أسماء الأعضاء وتواريخ ميلادهم، فتوقعوا تصيّداً احتيالياً يستشهد بها.**

4.7 ما تضيفه المنتديات

أسهمت المنتديات بـ 381 منشوراً موسوماً فقط، لكنها تحمل جميع الادعاءات الخاصة بمؤسسات بعينها تقريباً (الحالات A-E). ولا تزال معظم نتائج المنتديات قوائم عملاء محتملين عالمية تذكر الإمارات ضمن عشرات البلدان. ونشر مشترون أيضاً طلبات: لبيانات نظام إدارة علاقات العملاء لوكالة عقارية (B20)، ولبيانات عملاء مشغّل مطار دولي، ولـ«قاعدة بيانات الهوية الإماراتية» في نوفمبر. والطلب على بيانات الهوية والعقارات في الإمارات نتيجة بحد ذاته.

الخلاصات الرئيسية

01

يغلب على الحجم الخام قوالب روبوتات متعددة البلدان؛ فاقرأ الأعداد بعد التنقية بوصفها حداً أعلى.

02

البيانات العقارية أكثر الفئات الخاصة بالإمارات عرضاً في المنشورات التي راجعناها؛ فهيّئ الملّاك لمواجهة احتيال تعليمات الدفع.

03

العروض ذات الطابع الحكومي في معظمها وصول واستطلاع وملفات معاد تداولها؛ فافحص المصدر قبل التعليق.

الفصل 5

أمثلة على الاستهداف بحسب القطاع

يجيب هذا الفصل عن

أي القطاعات في دولة الإمارات تُذكر في المنشورات الإجرامية ومنشورات ناشطي القرصنة، وما نوع الاستجابة التي يحتاجها كل منها؟

10

قطاعات رُصد فيها نشاط، من الحكومة إلى العقارات

باختصار

تُظهر المنشورات أدناه كيف تتحدث الجهات الإجرامية وناشطو القرصنة عن المؤسسات الإماراتية. ذكر ناشطو القرصنة أهدافاً حكومية بارزة وأخرى في قطاعي الطاقة والنقل، وادّعوا إحداث تعطيل. وذكر البائعون الإجراميون بيانات في العقارات والتأمين والتعليم والنقل، وتعاملوا مع الإمارات بوصفها سوقاً للحسابات والهويات. وتُذكر التقارير الرسمية بشكل منفصل. تحقّق من كل ادعاء مع الجهة المذكورة قبل التصعيد، وابدأ بالاستجابة الأولى الخاصة بالقطاع.

يُوصف الضحايا بأدوارهم وفق السياسة الواردة في الملحق A.9، إلا إذا أُكّدت الحادثة رسمياً ونُقلت على نطاق واسع. وتأتي الأمثلة من المجموعة المنقّاة، ومنشورات المنتديات التي تذكر الإمارات، والتقارير العامة. والاستجابات الأولى نقاط بداية؛ أما الإجراءات المُسندة، مع الجهات المسؤولة وأدلة الإنجاز، فهي في §12.18 (الصفوف 2–4 و 6 و 14–19).

الحكومة

ادعاء DDoS، ادعاء تدميري، بيع وصول، استطلاع، أسطر بيانات اعتماد

مثال على نشاط مرصود (بعد إخفاء الهوية)

ادعاءات DDoS ضد مواقع حكومية اتحادية (مارس–أبريل، الفصل 6)؛ ادعاء اختراق وتسريب ومسح تدميري ضد عدة جهات من القطاع العام في إمارة واحدة (أبريل، غير مؤكد)؛ وصول بصلاحيات مدير أعلى إلى نظام دائرة مالية مقابل 800 USD (أبريل)؛ استطلاع لمنظومة ذكاء اصطناعي (مارس)؛ أسطر بيانات اعتماد لصفحة دخول خدمات إلكترونية حكومية (أغسطس)؛ إدراجان ضد هيئة نقل (أبريل، نوفمبر)

ما يعنيه

الإتاحة وسلامة بيانات المواطنين ووصول المديرين هي أوجه الانكشاف الثلاثة

الاستجابة الأولى

الاتفاق مسبقاً على بيانات حالة الخدمة؛ فرض تسجيل الدخول الموحّد والمصادقة متعددة العوامل على واجهات الإدارة

العقارات

بيع بيانات، تسريب، ادعاء تدميري

مثال على نشاط مرصود (بعد إخفاء الهوية)

تسع مجموعات بيانات على الأقل لملّاك ومستأجرين ومطوّرين وبوابات (يناير–نوفمبر)؛ مشترٍ يبحث عن نظام إدارة علاقات عملاء لوكالة (فبراير)؛ ادعاء مسح ضد منصة عقارية (سبتمبر)

ما يعنيه

أكثر البيانات الخاصة بالإمارات عرضاً في المنشورات التي راجعناها؛ تغذّي احتيال تعليمات الدفع والتسليم

الاستجابة الأولى

مراجعة صادرات أنظمة إدارة علاقات العملاء ووصول الشركاء؛ تحذير الملّاك من طلبات تغيير بيانات الدفع

البنوك والمدفوعات

الاحتيال بالبطاقات، الحسابات الوسيطة، التسييل، بيانات الاعتماد

مثال على نشاط مرصود (بعد إخفاء الهوية)

مخرجات فحص بطاقات تذكر 14 جهة إصدار إماراتية (ذروة في فبراير–مارس)؛ وثائق هوية لحضور مؤتمر مالي تُركت مكشوفة في مساحة تخزين لدى مورّد، وأكّدت الجهة المنظِّمة ذلك وأمّنت المساحة (فبراير) [S65]؛ تجنيد حسابات وسيطة لتمرير الأموال (mule) لحسابات تجارية وشخصية في بنوك مسمّاة؛ تسييل عبر روابط الدفع وأجهزة نقاط البيع؛ أسطر بيانات اعتماد لتسجيل الدخول إلى بنك للأفراد

ما يعنيه

تهيمن أدوات الاحتيال؛ ويكمن الانكشاف المتصل بالاختراق في بيانات الأجهزة (الفصل 9)

الاستجابة الأولى

فرز إدراجات بيانات الاعتماد الحالية، ثم أجهزة الموظفين؛ مراقبة التجار بحثاً عن أنماط التسييل

الطاقة والمرافق

ادعاء تسريب، ادعاء DDoS، ادعاء يخص التقنيات التشغيلية (OT)

مثال على نشاط مرصود (بعد إخفاء الهوية)

ادعاء تسريب بحجم 1.3 TB ضد شركة نفط في إحدى الإمارات أُعيد نشره (مارس)؛ قوائم DDoS تذكر شركة نفط وغاز ومرفق خدمات (مارس)؛ ادعاء غير محدد باختراق «أنظمة الكهرباء» (يونيو)

ما يعنيه

يذكر تحذير المجلس بشأن برمجيات المسح التدميرية (wiper) قطاع الطاقة ضمن القطاعات المستهدفة [S11]

الاستجابة الأولى

التحقق من ادعاءات التقنيات التشغيلية مع مالك النظام؛ اختبار النسخ الاحتياطية غير المتصلة والاستجابة لبرمجيات المسح

النقل والطيران

ادعاء وصول غير مصرح به، إدراج في موقع تسريب، إعادة بيع حسابات

مثال على نشاط مرصود (بعد إخفاء الهوية)

ادعاء أُعيد نشره بالوصول إلى مشغّل مطار دولي (مارس، وتكرر في أغسطس)؛ ادعاء يخص ميناء (مايو)؛ إدراجات ابتزاز ضد شركة تموين جوي وشركة طيران منخفض التكلفة (أغسطس، أكتوبر)؛ إعادة بيع حسابات أميال الولاء

ما يعنيه

بيانات المسافرين ووثائق الهوية هي الانكشاف الجوهري

الاستجابة الأولى

مراقبة حسابات الولاء والعملاء؛ مراجعة بيانات اعتماد الشركاء وأنظمة الحجز

التأمين

بيع بيانات

مثال على نشاط مرصود (بعد إخفاء الهوية)

ملف من 80,000 سجل لعملاء ووسطاء نُشر على تيليغرام وفي ثلاثة منتديات (يناير–أبريل؛ الحالة A)

ما يعنيه

تفاصيل الوثائق والمدفوعات تجعل التصيّد الموجّه للعملاء مقنعاً

الاستجابة الأولى

مراجعة سجلات الوصول إلى نظام إدارة علاقات العملاء؛ إعداد إشعارات العملاء

التعليم

بيانات معاد تداولها، ادعاءات بيانات، إدراجات برامج الفدية

مثال على نشاط مرصود (بعد إخفاء الهوية)

إعادة نشر مجموعة بيانات طلابية من 2025 (يناير–مايو)؛ ادعاءات بتفريغ نظام إدارة مدرسية ومجموعات جوازات سفر ضد مجموعات مدارس؛ ثمانية إدراجات في مواقع التسريب ضمن قطاع التعليم

ما يعنيه

بيانات الطلاب وأولياء الأمور تدعم التصيّد الاحتيالي والاحتيال على الهوية

الاستجابة الأولى

فحص حقول بيانات الاعتماد في مجموعات البيانات القديمة؛ إعادة التعيين حيث أُعيد استخدامها

الرعاية الصحية

ادعاء بيع بيانات، إدراج ابتزاز

مثال على نشاط مرصود (بعد إخفاء الهوية)

بيع ملفات منسوبة إلى هيئة الصحة في إحدى الإمارات أُعيد نشره (أبريل)؛ إدراجات في موقع تسريب تذكر ثلاث مجموعات مستشفيات من مجموعة لم نتمكن من تأكيد إدراجاتها (فبراير)

ما يعنيه

المعرّفات الصحية لا تنتهي صلاحيتها؛ تحقّق قبل الإشعار

الاستجابة الأولى

مقارنة البنى المدّعاة بالأنظمة الفعلية قبل أي إشعار

التجزئة والاستهلاك

حادثة مؤكدة، إدراج، بيع وصول

مثال على نشاط مرصود (بعد إخفاء الهوية)

حادثة مؤكدة في برنامج ولاء لدى Landmark Group وإدراج في موقع تسريب في الأسبوع نفسه (نوفمبر؛ الحالة F)؛ عرض وصول إلى منصة بقالة مقابل 100 USD (يونيو)

ما يعنيه

منصات الولاء أنظمة هوية

الاستجابة الأولى

حماية وصول مديري منصات الولاء بالمصادقة متعددة العوامل؛ مراقبة عمليات التصدير بالجملة

الاتصالات

خدمات SIM، التصيّد الاحتيالي، ادعاء بيانات

مثال على نشاط مرصود (بعد إخفاء الهوية)

بيع شرائح SIM وأرقام افتراضية بمفتاح +971؛ أداة تصيّد احتيالي تستهدف مشغّلاً وطنياً؛ ادعاء غير مدعوم بقاعدة بيانات لمشغّل من 7 ملايين سجل

ما يعنيه

خدمات SIM والأرقام مرتبطة بالاحتيال عبر استعادة الحسابات

الاستجابة الأولى

تشديد ضوابط تبديل شرائح SIM ونقل الأرقام (§12.18 الصف 18)

قراءة عبر القطاعات. تنقسم الادعاءات الخاصة بمؤسسات بعينها إلى مجموعتين. ذكر ناشطو القرصنة أهدافاً بارزة (بوابات الدولة، والطاقة، والموانئ والمطارات)، وادّعوا إحداث تعطيل أو تدمير، وتركّز معظم نشاطهم في مارس وأبريل. أما البائعون ذوو الدوافع المالية فذكروا بيانات العقارات والتأمين والنقل، وتعاملوا مع الإمارات في ما عدا ذلك بوصفها سوقاً للحسابات والهويات المُتحقق منها. وكانت المجموعة الثانية نشطة طوال العام، وهي أقل ظهوراً في الصحافة.

الخلاصات الرئيسية

01

ذكر ناشطو القرصنة أهدافاً حكومية بارزة وأخرى في قطاعي الطاقة والنقل، معظمها في مارس-أبريل.

02

كانت العقارات أكثر فئات البيانات الخاصة بالإمارات عرضاً في المنشورات التي راجعناها.

03

بالنسبة للبنوك وشركات الاتصالات، تشير المنشورات إلى ضوابط فتح الحسابات والحسابات الوسيطة وشرائح SIM أكثر مما تشير إلى الاختراق.

الفصل 6

نشاط ناشطي القرصنة وهجمات حجب الخدمة الموزعة (DDoS) والادعاءات التدميرية

يجيب هذا الفصل عن

من ادّعى تنفيذ هجمات على أهداف في دولة الإمارات في 2026، وماذا قالت الجهات الرسمية، وكيف ينبغي للمؤسسة أن تستعد للادعاء التالي؟

10

ادعاءات DDoS في منشورات الجهات الفاعلة التي قرأناها ضد أهداف إماراتية، جميعها بين 2 مارس و 8 أبريل

في هذا الفصل

6.1 التسلسل الزمني

6.2 مارس-أبريل: ادعاءات DDoS قصيرة وكثيرة

6.3 ادعاءات التدمير والاختراق والتسريب: الادعاء مقابل الرواية الرسمية

6.4 دروس لفرق الدفاع

باختصار

تركّزت ادعاءات ناشطي القرصنة (هاكتيفست) ضد الإمارات في مارس وأبريل، خلال فترة التصعيد التي وصفتها الجهة الوطنية المعنية بالأمن السيبراني. وكان معظمها ادعاءات DDoS قصيرة ضد مواقع اتحادية ومحلية، لا يسندها سوى روابط فحص الإتاحة. أما ادعاءات الاختراق والتسريب والمسح التدميري الأكبر ضد جهات حكومية وشركة نفط وميناء ومطار، فلم تصلنا إلا عبر إعادة النشر، ولم تؤكدها الجهات المذكورة. اتفق مسبقاً على من يؤكد حالة الخدمة، واختبر النسخ الاحتياطية غير المتصلة.

6.1 التسلسل الزمني

18 فبراير 2026

مجلس الأمن السيبراني لحكومة دولة الإمارات

128 حادثة مؤكدة منذ 1 يناير؛ تشويه المواقع 38.3% وتسريبات البيانات 25.8% من الإجمالي

22 فبراير 2026

RipperSec

يدّعي تسريب قواعد بيانات أربع شركات إماراتية

28 فبراير 2026

مجلس الأمن السيبراني لحكومة دولة الإمارات

بداية فترة التصعيد التي وصفها لاحقاً رئيس المجلس (حتى مطلع أبريل)

2 مارس 2026

Team 313

يدّعي هجوم DDoS لمدة ساعة على موقعين حكوميين اتحاديين؛ وادعاءات أخرى حتى 11 مارس ضد عدة جهات اتحادية

3 مارس 2026

روبوتات رصد التسريبات

تعيد نشر ادعاء Handala بالحصول على 1.3 TB من شركة نفط في إحدى الإمارات

6 مارس 2026

DieNet (رسالة من روبوتها، أُعيد نشرها)

ادعاءات DDoS ضد مواقع حكومية اتحادية

9 مارس 2026

+Keymous

أول قائمة أهداف DDoS إماراتية؛ ستة مواقع اتحادية مع روابط فحص الإتاحة في 12 مارس؛ وقوائم أخرى حتى 8 أبريل، منها مواقع طاقة ومرافق

19 مارس 2026

مجلس الأمن السيبراني لحكومة دولة الإمارات

تحذير علني من برمجيات المسح التدميرية (wiper) (تقرير صحفي حُدّث في 19 مارس)

27 مارس 2026

coderx

ينشر قاعدة بيانات بحجم 16.6 GB ينسبها إلى شركة لإدارة المرافق في دبي

30 مارس 2026

قنوات الرصد

تعيد نشر ادعاء Nasir Security بالوصول إلى مشغّل مطار دولي، مع صور جوازات سفر بحسب الادعاء

4 أبريل 2026

مجلس الأمن السيبراني لحكومة دولة الإمارات

تحذير من حملة مسح تدميري (wiper) عبر القطاعات؛ «بعض المؤسسات تأثرت بالفعل»

12 أبريل 2026

الصحافة الأمنية

Handala يدّعي مسحاً تدميرياً وسرقة بيانات لدى عدة جهات من القطاع العام في إمارة واحدة: تدمير 6 PB وسرقة 149 TB

4 مايو 2026

قنوات متوافقة معه

تعيد نشر ادعاء Handala ضد ميناء في إحدى الإمارات

1 يونيو 2026

Golden Falcon

يدّعي أنه بدأ اختراقاً لأنظمة الكهرباء في الإمارات

10 سبتمبر 2026

حساب تجميع

يدّعي تصدير قاعدة بيانات منصة عقارية إماراتية بحجم 49 GB وحذفها

15 سبتمبر 2026

رئيس مجلس الأمن السيبراني لحكومة دولة الإمارات

مخترق استغل ثغرة غير مُعالَجة وطالب مؤسسة من القطاع الخاص بـ 5 ملايين USD

18 نوفمبر 2026

رئيس مجلس الأمن السيبراني لحكومة دولة الإمارات

أكثر من 40 مجموعة من أكثر من 20 دولة حاولت استغلال الأزمة الإقليمية

العلامات الداكنة منشورات لجهات فاعلة، والعلامات المحددة بإطار إعادة نشر من أطراف ثالثة، والعلامات المرجانية بيانات رسمية. التواريخ هي تواريخ المنشورات أو البيانات. المصادر: منشورات الجهات الفاعلة وإعادة نشرها [S1]؛ البيانات الرسمية [S9][S12] [S11][S17][S22]؛ ادعاء Handala في أبريل [S26].

6.2 مارس-أبريل: ادعاءات DDoS قصيرة وكثيرة

كانت ادعاءات DDoS قصيرة وعلنية وضعيفة الأدلة. لدينا 22 منشوراً لجهات فاعلة تدّعي تنفيذ أعمال ضد أهداف إماراتية. وفي المنشورات التي قرأناها، تقع ادعاءات DDoS العشرة جميعها بينها في الفترة بين 2 مارس و 8 أبريل، وصدرت عن Team 313 وKeymous+ وCyber Fattah. ولم تصلنا ادعاءات DieNet إلا عبر إعادة نشر رسائل الروبوت الخاصة بها (اعتباراً من 1 مارس)، وهي ليست ضمن الادعاءات العشرة. وكانت الأهداف مواقع حكومية اتحادية، ومواقع حكومية ومكاتب إعلامية في الإمارات المحلية، ومواقع طاقة ومرافق، والموقع العام لبنك واحد. وكان الدليل المقدَّم روابط فحص الإتاحة: لقطات لإمكانية الوصول من عدد قليل من مواقع الفحص. وقد تسجّل هذه الروابط لحظة تعذّر وصول، لا انقطاعاً في الخدمة.

بطاقة الدليل B21 — 2 مارس 2026

Team 313 قناة الجهة الفاعلة · Telegram · العربية، الإنجليزية

النص الأصلي

هجوم سيبراني استهدف خوادم الرئيسية لحكومة الامارات حيث ادى الهجوم الى تعطل [موقع حكومي اتحادي 1] و[موقع حكومي اتحادي 2] [...] سيستمر الهجوم لمدة ساعة كاملة.

ملاحظة. واحد من أربعة ادعاءات لـ Team 313 (11-2 مارس) ضد مواقع حكومية اتحادية ومحلية.

ما يمكن إثباته	ادّعت المجموعة تنفيذ هجوم حجب خدمة موزع (DDoS) لمدة ساعة على موقعين حكوميين اتحاديين في 2 مارس.
ما لم يثبت	لا يثبت ذلك أي انقطاع يتجاوز روابط Check-Host التي نشرتها الجهة الفاعلة نفسها.

بطاقة الدليل B22 — 12 مارس 2026

Keymous+ قناة الجهة الفاعلة · Telegram · الإنجليزية

النص الأصلي

```
United Arab Emirates : [federal
government website] Check Host [...]
[federal ministry 1] Check Host [...]
[federal ministry 2] Check Host [...]
[federal ministry 3] Check Host [...]
[federal ministry 4] Check Host [...]
[federal ministry 5] Check Host
```

الترجمة

الإمارات العربية المتحدة : [موقع حكومي اتحادي] Check Host [...] [وزارة اتحادية 1] Check Host [...] [وزارة اتحادية 2] Check Host [...] [وزارة اتحادية 3] Check Host [...] [وزارة اتحادية 4] Check Host [...] [وزارة اتحادية 5] Check Host

ملاحظة. نشرت Keymous+ خمس قوائم أهداف إماراتية على الأقل بين 9 مارس و8 أبريل، منها شركة نفط وغاز ومرفق خدمات.

ما يمكن إثباته	أدرجت Keymous+ ستة مواقع حكومية اتحادية أهدافاً لهجمات DDoS، وقدّمت روابط Check-Host دليلاً.
ما لم يثبت	لا يثبت ذلك أي أثر على الخدمة، إذ تلتقط نتائج Check-Host لحظة واحدة من مواقع فحص قليلة.

ويؤكد القياس المستقل زيادة في هجمات DDoS، معظمها منخفض الحجم. أفادت StormWall بأن حصة الإمارات من نشاط DDoS في المنطقة ارتفعت من 14% إلى 26% بين الربع الأول من 2025 والربع الأول من 2026. وقدّرت ارتفاع الهجمات على الإمارات بنسبة 86% على أساس سنوي [S30]. وأحصت Help AG وقوع 236,560 هجوم DDoS على الشبكات الإماراتية في النصف الأول من 2026، 91% منها منخفض الحجم [S35]. ولم يُفِد أي من المصدرين بانقطاع وطني مستمر.

6.3 ادعاءات التدمير والاختراق والتسريب: الادعاء مقابل الرواية الرسمية

جاءت أخطر الادعاءات من Handala، وهي علامة تصفها Security Affairs بأنها تقدّم نفسها مجموعةً لناشطي القرصنة مؤيدةً للفلسطينيين، وبأنها يُنظر إليها على نطاق واسع كواجهة لجهة فاعلة مدعومة من إيران [S26]. ولم تصل منشوراتها إلى بياناتنا إلا عبر إعادة النشر.

النقطة	ادعاء Handala (12- أبريل 13)	الرواية الرسمية	التقارير المستقلة
الأهداف	عدة جهات من القطاع العام في إمارة واحدة	لم نعثر على بيان يتناول الادعاء حتى تاريخ الإقفال لدينا	الادعاءات «لا تزال غير مُتحقق منها» [S26]
الأثر	تدمير 6 PB من البيانات	وصف تحذير المجلس الصادر في 4 أبريل حملة مسح تدميري إقليمية نشطة دون تسمية ضحايا [S11]	لم يُقَس
البيانات	سرقة 149 TB	غير مذكور	لم يُتحقق منه [S26]
الإسناد	ادعاء ذاتي	أدلى رئيس المجلس بتصريحات إسناد في مناسبات أخرى (§2.4)	واجهة لجهة فاعلة مدعومة من إيران، كما وصفتها Security Affairs [S26]

ما يمكننا إثباته. ادّعت علامة تربطها Security Affairs بجهة فاعلة مدعومة من إيران [S26] تنفيذ هجوم مسح تدميري على جهات حكومية، وكانت الجهة الوطنية قد حذّرت من حملة مسح تدميري نشطة قبل ذلك بثمانية أيام. والأحجام المدّعاة كبيرة جداً بالنسبة لجهات من هذا النوع، ولم تؤكد أي جهة مذكورة وقوع حادثة حتى تاريخ الإقفال لدينا. ونحن لا نحسب نسبة بين الادعاء والواقع ولا نلمّح إليها.

وتكرر النمط نفسه في الادعاءات الكبيرة الأخرى. ادّعى Handala الحصول على 1.3 TB من شركة نفط في إحدى الإمارات (3 مارس)، وعلى بيانات من ميناء (4 مايو). وادّعت Nasir Security وصولاً استمر أشهراً إلى مشغّل مطار دولي (30 مارس، وتكرر في أغسطس)، كما ادّعت استهداف جهة جمركية (أغسطس) [S66]. وأُعيد نشرها جميعاً، لكن الجهات المذكورة لم تؤكدها حتى تاريخ الإقفال لدينا. وأوردت جهات رصد عامة ادعاءَي الميناء والمطار بوصفهما مزاعم [S27][S28].

حالة القطاع الخاص التي وصفتها الجهات الرسمية فعلاً. في 15 سبتمبر قال رئيس المجلس إن مخترقاً استغل ثغرة غير مُعالَجة لدى مؤسسة من القطاع الخاص لم يُكشف اسمها، وادّعى الوصول إلى أنظمتها، وهدّد بكشف بياناتها، وطالب بمبلغ 5 ملايين USD. وأفادت Khaleej Times بأن بعض المعلومات نُشرت لاحقاً على الويب المظلم؛ بينما أفادت Gulf News بأن التسريب مُنع [S17][S67]. ولم يُكشف اسم المؤسسة.

بطاقة الدليل B23 — 27 مارس 2026

coderx منتدى تسريبات · Forum · الإنجليزية

النص الأصلي

```
16GB [Dubai facilities-management company] DATABASE [...] Leaking 16GB Database Of [Dubai facilities-management company] [...] Number Of Files: 1 Original Size: 16.6 GB Compressed Size: 696 MB
```

الترجمة

قاعدة بيانات [شركة إدارة مرافق في دبي] بحجم 16GB [...] تسريب قاعدة بيانات بحجم 16GB لـ [شركة إدارة مرافق في دبي] [...] عدد الملفات: 1 الحجم الأصلي: 16.6 GB الحجم المضغوط: 696 MB

ملاحظة. حُذفت هنا التصريحات السياسية الواردة في المنشور.

ما يمكن إثباته

نشرت جهة فاعلة قاعدة بيانات بحجم 16.6GB نسبتها إلى شركة إدارة مرافق في دبي.

ما لم يثبت

لا يثبت ذلك أن الملف هو ما تقوله الجهة الفاعلة.

بطاقة الدليل B24 — 1 يونيو 2026

Golden Falcon قناة الجهة الفاعلة · Telegram · الإنجليزية

النص الأصلي

```
The attack on the UAE's electricity systems has begun [...] It was just a small warning, and this time we just agreed to read the data
```

الترجمة

بدأ الهجوم على أنظمة الكهرباء في الإمارات [...] كان مجرد تحذير صغير، وهذه المرة اكتفينا بقراءة البيانات

ملاحظة. أعادت قناة رصد نشره في اليوم التالي، ولا متابعة له في مجموعة البيانات المرصودة.

ما يمكن إثباته

ادّعت مجموعة أنها بدأت عملية تسلل إلى أنظمة الكهرباء في الإمارات، وأنها اكتفت بقراءة البيانات.

ما لم يثبت

لا يسمّي ذلك أي مشغّل أو نظام، ولا يقدّم دليلاً، ولا يثبت أي أثر على إمدادات الكهرباء.

وجاء الادعاء الوحيد من نوع المسح التدميري ضد شركة إماراتية في بياناتنا لاحقاً، في سبتمبر، من جهة فاعلة قالت إنها صدّرت قاعدة بيانات منصة عقارية ثم حذفتها (B05). ولم يعقب ذلك انقطاع أو تأكيد في المصادر التي راجعناها.

بطاقة الدليل B05 — 10 سبتمبر 2026

حساب تجميعي (معرّف الجهة الفاعلة محجوب)

منتدى لتجميع التسريبات · Forum · الإنجليزية

النص الأصلي

```
49GB of [UAE real-estate platform]
Database Leaks [...] today I [contact
removed] gained access to a database
of a real estate company in the
United Arab Emirates. After exporting
the entire database i also wiping
everything out.
```

الترجمة

49GB من تسريبات قاعدة بيانات [منصة عقارية إماراتية] [...] اليوم أنا [تمت إزالة جهة الاتصال] حصلت على وصول إلى قاعدة بيانات شركة عقارية في الإمارات العربية المتحدة. وبعد تصدير قاعدة البيانات بالكامل قمت أيضاً بمسح كل شيء.

ملاحظة. هذا هو الادعاء الوحيد من نوع برمجيات المسح التدميرية (wiper) ضد شركة إماراتية في مجموعة البيانات المرصودة.

ما يمكن إثباته	ادّعت جهة فاعلة أنها صدّرت قاعدة بيانات بحجم 49GB لمنصة عقارية إماراتية ثم حذفتها.
ما لم يثبت	لا يثبت ذلك حدوث أي حذف، ولا أن المنصة فقدت الخدمة.

6.4 دروس لفرق الدفاع

1. **استعد لبرمجيات المسح التدميرية، لا للتشفير وحده.** يصف تحذير المجلس نفسه برمجيات خبيثة تدميرية تدخل عبر التصيّد الاحتيالي وبيانات اعتماد VPN المسروقة والأنظمة غير المحدّثة [S11]. اختبر أن النسخ الاحتياطية غير المتصلة تُستعاد خلال زمن الاستعادة الذي التزمت به (§12.1 الصفوف 4 و6 و17).
2. **اتفق مسبقاً على الموقف العلني.** صُمّمت أرقام ناشطي القرصنة لكي تُقتبس. حدّد مسبقاً من يؤكد حالة الخدمة، وخلال أي مدة، وعبر أي قناة (§12.1 الصف 16).
3. **احمِ البوابات من المنبع.** تستهدف ادعاءات DDoS القصيرة والمتكررة البوابات العامة. تعاقد على خدمات التخفيف لدى مزوّد المنبع قبل فترة التصعيد التالية (§12.1 الصف 9).
4. **تحقّق من ادعاءات التقنيات التشغيلية قبل التصعيد.** ادعاء الوصول إلى «أنظمة الكهرباء» دون تسمية مالك النظام سبب للتحقق، لا للإعلان ([B24]؛ §12.1 الصف 16).

الخلاصات الرئيسية

01

تركّزت ادعاءات DDoS من ناشطي القرصنة في مارس-أبريل واستندت إلى روابط فحص الإتاحة.

02

بقيت ادعاءات التدمير والاختراق والتسريب ضد جهات حكومية وقطاع الطاقة وميناء ومطار غير مؤكدة من الجهات المذكورة.

03

يحدد تحذير الجهة الوطنية نفسها بشأن المسح التدميري الضوابط: الدفاع ضد التصيّد الاحتيالي، وسلامة بيانات اعتماد VPN، والتحديث، ونسخ احتياطية قابلة للاستعادة.

الفصل 7

الجهات الفاعلة في التهديد

يجيب هذا الفصل عن

ما أنواع الجهات الفاعلة المهمة لدولة الإمارات، وكيف ترتبط ببعضها، وماذا تقول التقارير العامة عن كل منها؟

4

أنواع من الجهات الفاعلة: التجسس المرتبط بدول، والاختراق والتسريب التدميري، وبرامج الفدية، وشبكات الاحتيال

في هذا الفصل

7.1 كيف ترتبط الجهات الفاعلة

7.2 التجسس المرتبط بدول

7.3 جهات الاختراق والتسريب التدميري وناشطو القرصنة (هاكتيفست)

7.4 برامج الفدية والابتزاز

7.5 شبكات الاحتيال والشخصيات الإجرامية

باختصار

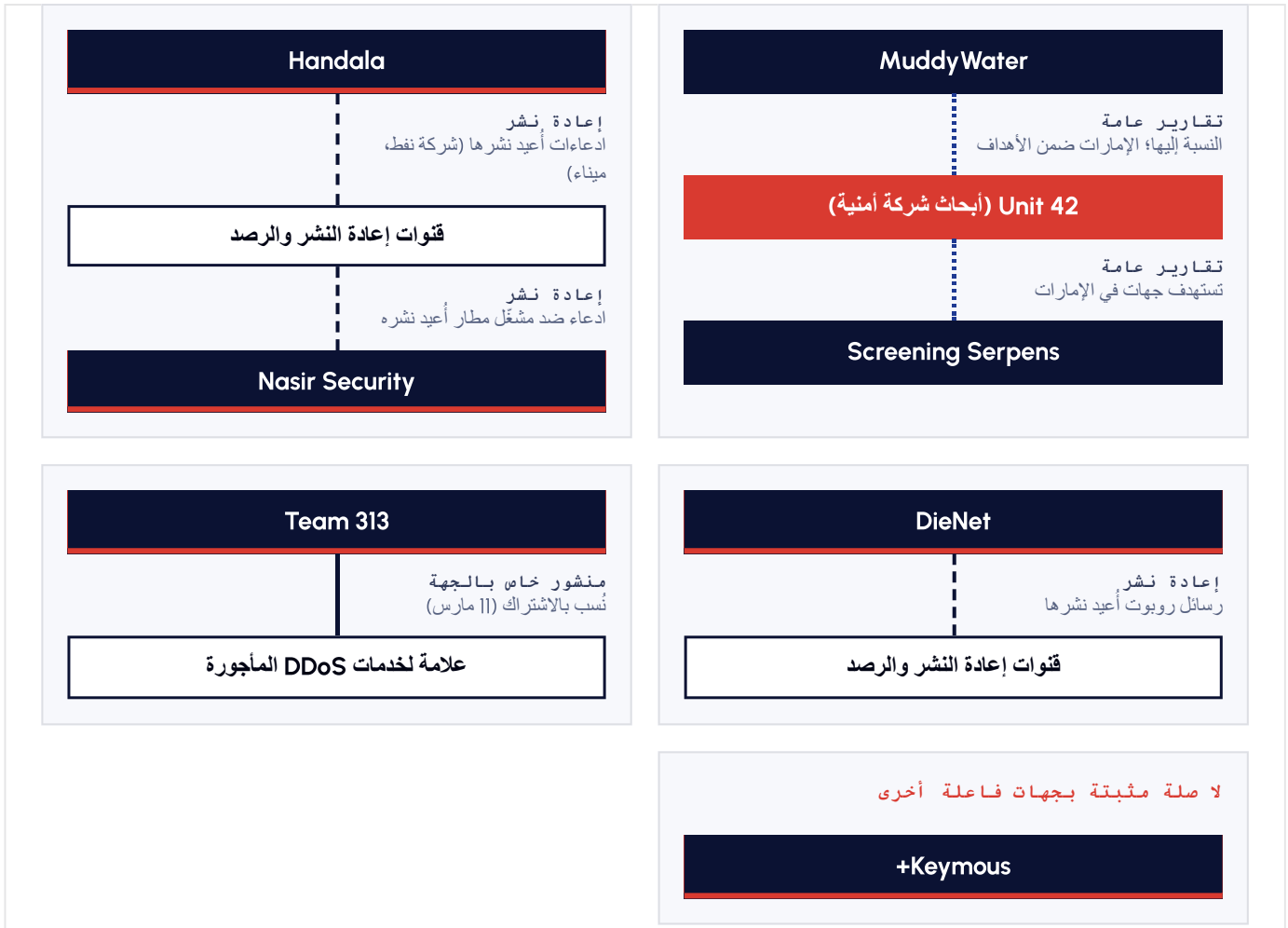
أربعة أنواع من الجهات الفاعلة مهمة لدولة الإمارات في عام 2026. أفادت شركات أمنية بأنشطة تجسس مرتبطة بدول استهدفت جهات إماراتية عبر التصيّد الاحتيالي وإغراءات التوظيف. وادّعت علامة للاختراق والتسريب تنفيذ هجمات تدميرية على جهات حكومية، ولم تؤكدها تلك الجهات. وأدرجت مجموعات برامج الفدية والابتزاز عشرات الشركات الإماراتية، أغلبها شركات خاصة. واستغلت شبكات الاحتيال قنوات الدفع والهوية في الدولة. رقّعوا الأنظمة الطرفية، وابحثوا عن ملفات DLL المحمّلة جانبياً وأدوات الإدارة عن بُعد وحركة الخروج غير المعتادة من خوادم البريد وCRM، وتحققوا من كل ادعاء قبل التعليق عليه.

يفصل كل ملف تعريفي بين **ما رصده المصدر**، و**الإسناد كما يذكره المصدر**، و**ما يبقى دون حسم**، و**ما يعنيه ذلك للمؤسسات**. تنطبق درجة الثقة على مقولة محددة، لا على الجهة الفاعلة ككل. الإسنادات هي إسنادات المصادر نفسها، ولا نقدّم أي إسناد من عندنا.

7.1 كيف ترتبط الجهات الفاعلة

تربط الخريطة بين الجهات الفاعلة فقط حيث نملك دليلاً، ويبيّن كل خط نوع ذلك الدليل: منشور الجهة نفسها، أو إعادة نشر من طرف ثالث، أو بيان رسمي، أو تقارير عامة. الخط يعني ارتباطاً، وليس دليلاً على وجود مشغّل مشترك.

منشور خاص بالجهة — إعادة نشر — بيان رسمي ..... تقارير عامة - - - ملاحظتنا



7.2 التجسس المرتبط بدول

MuddyWater (Boggy Serpens)

Boggy Serpens (التسمية لدى Unit 42)

تجسس (مرتبط بدولة بحسب الشركة الأمنية)

نسبتها Unit 42 إلى وزارة الاستخبارات والأمن في إيران

تقارير متصلة بالإمارات، 2026

يناير-فبراير	موجة ضد شركة بحرية وطاقة في الشرق الأوسط، واستخدم أحد الطُعوم سجلات رواتب بالدرهم
مارس	تدرج Unit 42 الإمارات ضمن الدول التي طالتها حملات حديثة

القطاعات المستهدفة

جهات حكومية ومؤسسية؛ شركة بحرية وطاقة في المنطقة

في التقارير العامة

- [S31] Unit 42 (16 مارس 2026): النسبة كما وردت؛ تصيّد احتيالي من حسابات بريد رسمية ومؤسسية مُستولى عليها؛ أدوات الإدارة عن بُعد (Atera وScreenConnect وSimpleHelp) في حملات سابقة؛ وبرمجيات زرع مخصّصة في 2025-26

تقييمنا

يتمثل الخطر المتصل بالإمارات في رسائل تصيّد احتيالي تُرسل من صناديق بريد موثوقة مُستولى عليها. وفي حملات سابقة تلتها أدوات إدارة عن بُعد مشروعة تندمج في حركة مرور تقنية المعلومات؛ وفي 2025-26 تفيد الشركة الأمنية ببرمجيات زرع مخصّصة.

درجة الثقة **نسبة من شركة أمنية؛ استهداف الإمارات بحسب ما ذكرته الشركة**

Screening Serpens

UNC1549، Smoke Sandstorm، Iranian Dream Job (بحسب Unit 42)

تجسس (مرتبط بدولة بحسب الشركة الأمنية)

مرتبطة بإيران، بحسب Unit 42 (ثقة متوسطة إلى عالية بأن الحملات تعود إلى هذه المجموعة)

تقارير متصلة بالإمارات، 2026

أبريل	متغير جديد ربما استهدف جهة في الإمارات
مايو	تفيد Unit 42 باستهداف جهات في الولايات المتحدة وإسرائيل والإمارات

القطاعات المستهدفة

جهات في الإمارات (القطاع غير منشور)

في التقارير العامة

- [S32] Unit 42 (22 مايو 2026): طُعوم توظيف ودعوات اجتماعات مزيفة؛ البرمجيتان الخبيثتان MiniUpdate وMiniJunk V2؛ التحميل الجانبي لمكتبات DLL واختطاف AppDomainManager

تقييمنا

طُعوم عروض عمل ودعوات اجتماعات تستهدف موظفين أفراداً. ويعتمد الكشف على بيانات القياس من نقاط النهاية لرصد مكتبات DLL المحمّلة جانبياً في مسارات قابلة للكتابة من المستخدم.

درجة الثقة **متوسطة إلى عالية (بحسب الشركة الأمنية)**

التقنيات المذكورة في أبحاث الشركات الأمنية، بحسب التكتيك

الوصول الأولي	القيادة والتحكم	التهرب الدفاعي	الاستمرارية / التهرب الدفاعي
(لم يُذكر معرّف) تصيّد احتيالي يُرسل من صناديق بريد رسمية ومؤسسية مُستولى عليها (Unit 42، MuddyWater)	T1219 برمجيات الوصول عن بُعد: ScreenConnect وAtera وSimpleHelp، في حملات سابقة (Unit 42، MuddyWater)	T1055.012 تفريغ العمليات (Process hollowing) (Unit 42، MuddyWater)	T1574.001 التحميل الجانبي لمكتبات DLL، وفق تسمية Unit 42 (Screening Serpens) T1574.014 اختطاف AppDomainManager (Unit 42، Screening Serpens)

معرّفات التقنيات كما وردت في روابط تقريري Unit 42 الصادرين في 16 مارس و22 مايو 2026. ولا يحمل صف التصيّد الاحتيالي معرّفاً في المصدر. [S12]

اختراق غير منسوب لشركة دفاعية. أفادت ESET باختراق شركة دفاعية في دولة الإمارات عبر خادم SmartOffice CRM، أعقبه استخدام أدوات مخصصة لما بعد الاستغلال وأدوات وكيل عكسي. وصنّفت ESET هذا النشاط ضمن مجموعات أقل شهرة وغير منسوبة [S33]. ولم يُنشر أي معرّف CVE لنقطة الدخول.

استُهدفت كاميرات مكشوفة على الإنترنت. أفادت Check Point بارتفاع حاد في محاولات استغلال كاميرات IP في الإمارات ودول خليجية أخرى اعتباراً من 28 فبراير، انطلاقاً من بنية تحتية تنسبها إلى جهات إيرانية [S58]. ومن الثغرات التي أبرزتها CVE-2017-7921 في كاميرات Hikvision وCVE-2021-33044 في أجهزة Dahua. ويقيّم NVD كلتيهما بدرجة 9.8، وكلتاهما مدرجة في قائمة CISA للثغرات المستغَلة فعلياً [S59][S60]. وتختلف البرامج الثابتة المتأثرة والمُصلَحة بحسب الطراز (الجدول أدناه) [S68][S69]. وتداولت قائمة مجانية بنحو 185,000 بث كاميرا إماراتي مكشوف في 5 مارس (B11)، ووصف رئيس المجلس في نوفمبر محاولات لاختراق كاميرات المنازل والمزارع والسيارات [S23]. رقّعوا واجهات إدارة الكاميرات أو أزيلوا انكشافها على الإنترنت (12.1§ الصف 5).

CVE	سلسلة المنتجات	البرامج الثابتة المتأثرة	البرامج الثابتة المُصلَحة
CVE-2017-7921	Hikvision DS-2CD2xx2F-I	V5.2.0 build 140721 إلى V5.4.0 build 160530	V5.4.5 build 170123 أو أحدث
CVE-2017-7921	Hikvision DS-2CD2xx0F-I	V5.2.0 build 140721 إلى V5.4.0 build 160401	V5.4.5 build 170123 أو أحدث

CVE	سلسلة المنتجات	البرامج الثابتة المتأثرة	البرامج الثابتة المُصلَحة
CVE-2017-7921	Hikvision DS-2CD2xx2FWD	V5.3.1 build 150410 إلى V5.4.4 build 161125	V5.4.5 build 170124 أو أحدث
CVE-2017-7921	Hikvision DS-2CD4x2xFWD	V5.2.0 build 140721 إلى V5.4.0 build 160414	V5.4.5 build 170228 أو أحدث
CVE-2017-7921	Hikvision DS-2CD4xx5	V5.2.0 build 140721 إلى V5.4.0 build 160421	V5.4.5 build 170302 أو أحدث
CVE-2017-7921	Hikvision DS-2DFx	V5.2.0 build 140805 إلى V5.4.5 build 160928	V5.4.9 build 170123 أو أحدث
CVE-2017-7921	Hikvision DS-2CD63xx	V5.0.9 build 140305 إلى V5.3.5 build 160106	V5.4.5 build 170206 أو أحدث
CVE-2021-33044	كاميرات Dahua من IPC-HX1XXX إلى HX8XXX وHUM7XXX	إصدارات بُنيت قبل يونيو 2021	برامج ثابتة لكل طراز بتاريخ يوليو 2021 أو أحدث، ومنها V2.820.0000000.33.R.210705 (HX1XXX)
CVE-2021-33044	قباب PTZ من Dahua، سلسلة SD (SD1A1، SD22، SD49، SD50، SD52C، SD6AL)	إصدارات بُنيت قبل يونيو 2021	V2.812.0000007.0.R.210706 أو أحدث
CVE-2021-33044	كاميرات Dahua الحرارية TPC	إصدارات بُنيت قبل يونيو 2021	برامج ثابتة لكل طراز بتاريخ يوليو 2021، ومنها V2.630.0000000.6.R.210707 (TPC-BF1241)
CVE-2021-33044	أجهزة الاتصال الداخلي VTO وVTH من Dahua	إصدارات بُنيت قبل يونيو 2021	V4.300.0000003.0.R.210714 (VTO75X95X)، V4.300.0000004.0.R.210715 (VTO65XXX)، V4.500.0000002.0.R.210715 (VTH542XH)

إصدارات Hikvision هي الواردة في نشرة ICS-CERT؛ وقد لا تقبل الأجهزة التي تعمل ببرامج ثابتة غير مرخّصة التحديث. طابقوا الطراز الدقيق مع النشرة؛ فلا يوجد إصدار واحد من البرامج الثابتة يُصلح جميع الطرازات [S68][S69].

ما يبقى دون حسم. هويات الضحايا والبيانات المأخوذة ومدة البقاء داخل الشبكات غير معلنة في أي من هذه الحالات. **المعنى.** طرق الدخول الشائعة هي حسابات بريد موثوقة جرى الاستيلاء عليها، وإغراءات التوظيف، وتطبيقات الأعمال المكشوفة على الإنترنت. أطلقوا تنبيهات عند ظهور أدوات جديدة للإدارة عن بُعد، وعند التحميل الجانبي لملفات DLL من مجلدات قابلة للكتابة من المستخدم، وعند الاتصالات الصادرة غير المعتادة من خوادم CRM والبريد (§12.1 الصفان 4 و 7).

7.3 جهات الاختراق والتسريب التدميري وناشطو القرصنة (هاكتيفست)

Handala

Handala Hack

قرصنة وتسريب (hack-and-leak)، وادعاءات تدميرية

تقدّم نفسها بوصفها مؤيدة للفلسطينيين؛ وتصفها Security Affairs بأنه يُنظر إليها على نطاق واسع كواجهة لجهة فاعلة مدعومة من إيران

2026 في الإمارات

3 مارس	ادعاء الاستيلاء على 1.3 TB من شركة نفط في إحدى الإمارات (عبر إعادة نشر)
12-13 أبريل	ادعاء مسح تدميري (wiper) وسرقة لدى عدة جهات من القطاع العام في إمارة واحدة: تدمير 6 PB وسرقة 149 TB
4 مايو	ادعاء ضد ميناء في إحدى الإمارات (عبر إعادة نشر)

الأهداف المُدّعاة

جهات حكومية، والطاقة، وميناء

في التقارير العامة

- [S26] Security Affairs (13 أبريل 2026): لا تزال ادعاءات أبريل غير مؤكدة؛ وتصف العلامة وصلاتها بحسب ما أُفيد
- [S27] صفحة أخبار لشركة أمنية (مايو 2026) أوردت ادعاء الميناء، مستندة فقط إلى ادعاءات المجموعة نفسها

تقييمنا

الجهة المدّعية الأخطر من حيث النية المعلنة. لم تؤكد الجهات المذكورة أياً من ادعاءاتها لعام 2026 المتعلقة بالإمارات حتى تاريخ الإغلاق لدينا. ولم تصل منشوراتها إلى بياناتنا إلا عبر إعادة النشر.

درجة الثقة **عالية بأن الادعاءات صدرت؛ الأثر غير مؤكد**

Nasir Security

Nasir Resistance

ادعاءات قرصنة وتسريب (hack-and-leak)

غير مثبت؛ تأطير المجموعة لنفسها سياسي

2026 في الإمارات

30-31 مارس	ادعاء وصول استمر أشهراً إلى مشغّل مطار دولي، مع ادعاء الحصول على صور جوازات سفر ووثائق داخلية (عبر إعادة نشر)
22 أغسطس	ادعاء متجدد ضد المشغّل نفسه
22 أغسطس	ادعاء ضد هيئة جمارك، نُشر في اليوم نفسه (S66)

الأهداف المُدّعاة

الطيران (مشغّل مطار)؛ هيئة جمارك

في التقارير العامة

- [S28] أورد موقع عام لرصد حوادث تسرب البيانات ادعاء مارس بوصفه ادعاءً غير مثبت

تقييمنا

جهة مدّعية تركّز على عدد قليل من الأهداف المرتبطة بالدولة، ولم تصل أدلتها إلى بياناتنا مباشرة. والادعاء سبب لمراجعة وصول الشركاء وأنظمة إدارة الوثائق، لا للإعلان عن اختراق.

درجة الثقة **ادعاء منقول عبر إعادة النشر؛ غير مؤكد**

Team 313

ناشطو قرصنة (هجمات DDoS)

تأطير ذاتي ديني وسياسي (بحسب The National)؛ أعلنت بنفسها استهداف ست دول منها الإمارات؛ ولم يُتحقق من صلات بدول (CloudSEK، عبر The National)

2026 في الإمارات

2 مارس	ادعاء هجوم DDoS لمدة ساعة على موقعين حكوميين اتحاديين (B21)
3 مارس	ادعاء هجوم DDoS على موقع المكتب الإعلامي لإحدى الإمارات
11 مارس	ادعاء هجوم DDoS على موقع حكومي اتحادي، نُسب بالاشتراك مع علامة لخدمات DDoS المأجورة

الأهداف المُدّعاة

مواقع حكومية اتحادية ومحلية

بكلماتهم

> *"سيستمر الهجوم لمدة ساعة كاملة."* B21

في التقارير العامة

- The National [S29] (2 مارس 2026): أعلنت المجموعة علناً أنها تستهدف الإمارات ضمن ست دول؛ ولم تتمكن CloudSEK من التحقق من صلات بدول

تقييمنا

جهة تكرر ادعاءات DDoS، وأدلتها روابط فحص التوفر. ولم تؤكد الجهة المستهدفة أو أي جهة رسمية أي انقطاع مُدّعى.

درجة الثقة **عالية بأنها ادّعت؛ الأثر غير مؤكد**

+Keymous

ناشطو قرصنة (هجمات DDoS) | غير مثبت

2026 في الإمارات

9 مارس	قائمة DDoS: وزارة اتحادية، وشركة نفط وغاز، ومرفق خدمات
12 مارس	ستة مواقع اتحادية أُدرجت مع روابط فحص التوفر (B22)
25 مارس	شركة نفط وغاز ومرفق خدمات ضمن قائمة طاقة تشمل عشر دول
6-8 أبريل	أربعة مواقع أخرى لوزارات اتحادية

الأهداف المُدّعاة

مواقع الوزارات الاتحادية والطاقة والمرافق

بكلماتهم

> "[موقع حكومي اتحادي]" B22 Check Host

في التقارير العامة

- لم نجد في مسحنا تقارير عامة موثوقة عن ادعاءاتها المتعلقة بالإمارات

تقييمنا

أكثر الجهات تكراراً لادعاءات DDoS ضد الإمارات في بياناتنا (خمس قوائم). ولا تتجاوز أدلتها لقطات فحص لحظية.

درجة الثقة **عالية بأنها ادّعت؛ الأثر غير مؤكد**

DieNet

ناشطو قرصنة (هجمات DDoS)

غير مثبت؛ ورد اسمها في التغطية الصحفية ضمن مجموعات تدّعي تنفيذ هجمات في المنطقة

2026 في الإمارات	الأهداف المُدّعاة
1-9 مارس: رسائل ادعاء آلية أعادت نشرها قنوات متوافقة معها: عدة مواقع حكومية اتحادية	مواقع حكومية اتحادية

في التقارير العامة

- [S29] The National (2 مارس 2026): ورد اسمها ضمن مجموعات تدّعي تنفيذ هجمات في المنطقة؛ ولم يُتحقق من الادعاءات بشكل مستقل

تقييمنا

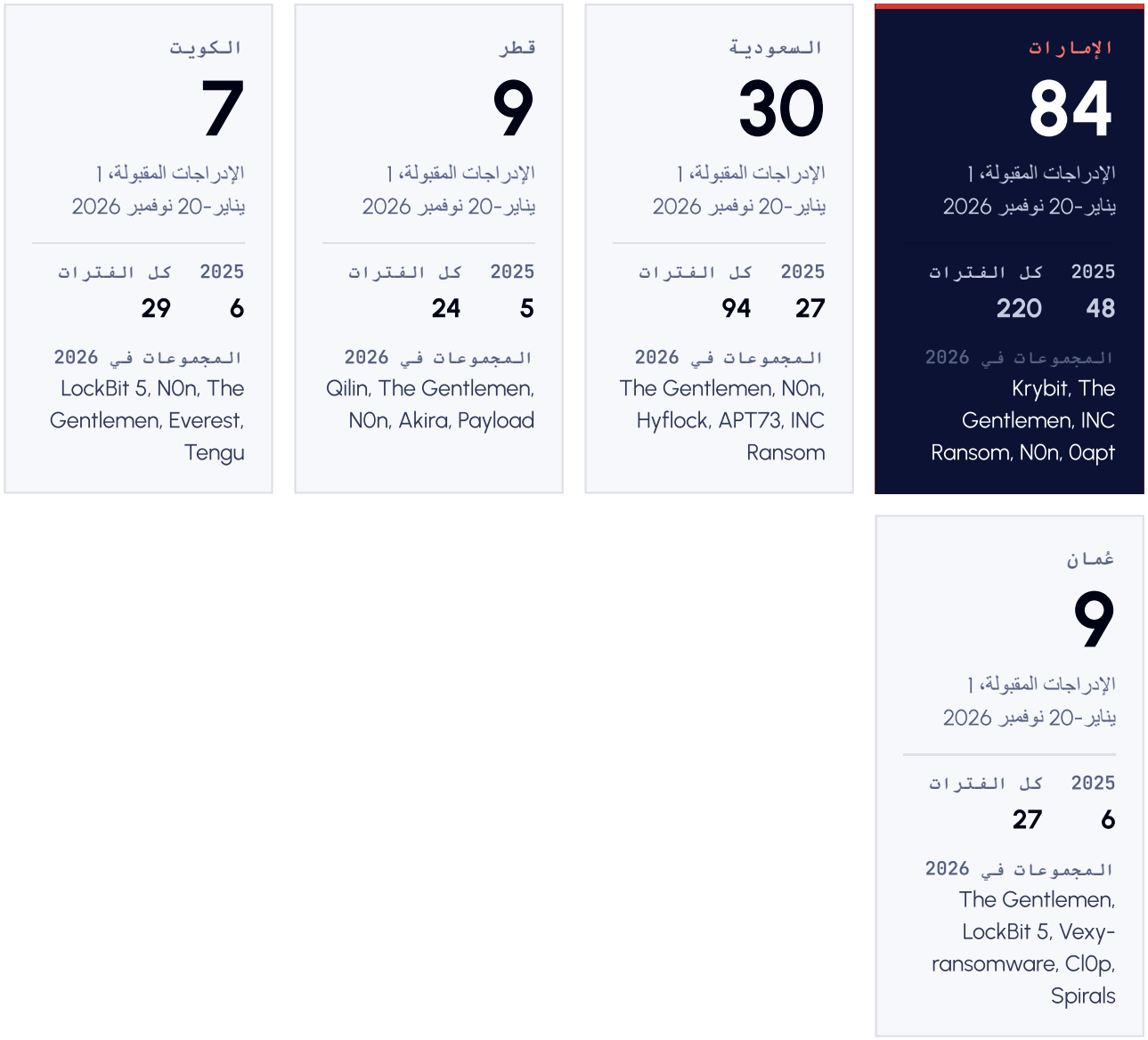
وصلتنا الادعاءات عبر إعادة نشر رسائل الروبوت الخاصة بالمجموعة، ولم يُؤكَّد أي منها.

درجة الثقة **ادعاء منقول عبر إعادة النشر؛ غير مؤكد**

نشرت جهات أخرى ادعاءات بوتيرة أقل. ادّعت RipperSec الحصول على قواعد بيانات أربع شركات إماراتية في فبراير، وادّعت Cyber Fattah استهداف موقع مصرف في مارس. وادّعت coderx الحصول على قاعدة بيانات لشركة إدارة مرافق في مارس، وادّعت Golden Falcon اختراق جهة كهرباء في يونيو. لم تؤكد الجهة المذكورة أو أي جهة رسمية أياً من هذه الادعاءات، ولم نجد تقارير عامة موثوقة تدعمها.

7.4 برامج الفدية والابتزاز

إدراجات برامج الفدية الإماراتية في 2026 تفوق بكثير إدراجات أربع دول خليجية للمقارنة



المصدر: الإدراجات المقبولة في Brandefense Ransompedia، جميع التواريخ، حتى 20 نوفمبر 2026 [S5]؛ وransomware.live للتحقق المتقاطع [S7].

إدراجات برامج الفدية والابتزاز متكررة وتسمّي في أغلبها شركات خاصة. تضم Ransompedia عدد 84 إدراجاً مقبولاً لدولة الإمارات مؤرخة بين ١ يناير و 20 نوفمبر 2026، مقابل 48 في عام 2025 بأكمله [S5]. خمسة من الإدراجات الـ 84 لا تخص مؤسسات ضحايا أو لا تقع بوضوح في الإمارات (مثل إعلان مجموعة عن قناتها الخاصة)، وخمسة تكرر مؤسسة مدرجة سابقاً، ليبقى 74 مؤسسة مختلفة. وسجّلت الدول الخليجية الأربع المستخدمة للمقارنة أعداداً أقل بكثير في الفترة نفسها: السعودية 30، وقطر 9، وعُمان 9، والكويت 7. وهذه أعداد إدراجات خام لدول المقارنة، لم تُنقَّ بالطريقة نفسها.

المقياس (الإمارات، 2026 حتى 20 نوفمبر)	القيمة
الإدراجات المقبولة	84 (74 مؤسسة إماراتية مختلفة مرجّحة)
المجموعات الأكثر نشاطاً	Krybit 8، The Gentlemen 7، INC Ransom 7، N0n 5، 0apt 4
القطاعات الأكثر ذكراً	التعليم 8، التجزئة 8، البناء 7، الاستشارات 7
الأشهر الأكثر نشاطاً	أكتوبر 13، ونوفمبر (حتى يوم 20) 12

الإدراج ادعاء إجرامي. أدرجت إحدى المجموعات ثلاث مجموعات مستشفيات وتكتلاً تجارياً في يوم واحد من فبراير. ولم نتمكن من تأكيد إدراجات هذه المجموعة، ولم تؤكد أي من تلك المؤسسات وقوع حادث. الإدراج الوحيد في 2026 الذي يمكننا مقارنته ببيان رسمي هو حالة برنامج ولاء التجزئة (الحالة F، §4.6). وتضع أرقام المجلس برامج الفدية عند 7.8% من 128 حادثاً مؤكداً حتى منتصف فبراير [S9]. إدراجات مواقع التسريب والحوادث المؤكدة تقيس أموراً مختلفة، لذا لا يمكن التوفيق بين الرقمين.

أدرج متتبع عام 70 ضحية موسومة بالإمارات خلال العام [S7]. عدد من وسومه، وبعض وسوم Ransompedia، يخص شركات مقرها في أماكن أخرى. حذفنا الإدخالات التي لا تخص بوضوح مؤسسات ضحايا في الإمارات، ولم نتحقق من كل وسم من الوسوم المتبقية.

7.5 شبكات الاحتيال والشخصيات الإجرامية

الشخصيات الإجرامية في بياناتنا هي في أغلبها بائعون يذكرون الإمارات سوقاً واحدة بين أسواق كثيرة. ونشرت مجموعة أصغر عروضاً خاصة بالإمارات. من بينهم بائع ملف شركة التأمين (الحالة A)، وبائعو مجموعات بيانات عقارية (الحالة C)، واسمان مستعاران وراء إدراجات هيئة النقل (الحالة B). وباع آخرون وصولاً ومعلومات استطلاع عن أنظمة حكومية (الحالة E)، وعرضت جهة واحدة قوائم سكانية (B10). ننشر الأسماء المستعارة كما نُشرت ونحجب وسائل الاتصال. لا يوجد عنصر ملموس مشترك يربط هذه الشخصيات ببعضها أو بعلامات ناشطي القرصنة. وأي تجميع لها سيكون نموذجاً تحليلياً، لا رصداً.

ولمجموعات الاحتيال خارج بيانات منشوراتنا أهمية أيضاً. تصف تقارير Recorded Future عن مجموعة Tajin إساءة استخدام بوابات دفع إماراتية في احتيال البطاقات وغسل الأموال [S34]. وفككت عمليات الشرطة في أبريل وأكتوبر مراكز احتيال وجمّدت آلاف الحسابات المصرفية (§8.5).

الخلاصات الرئيسية

01

أفادت شركات أمنية بأنشطة تجسس مرتبطة بدول استهدفت جهات إماراتية عبر حسابات بريد مستولى عليها وإغراءات التوظيف.

02

بقيت ادعاءات الاختراق والتسريب التدميري ضد جهات حكومية غير مؤكدة من تلك الجهات، فاستعدوا للتحقق قبل التعليق.

03

تسمّي إدراجات برامج الفدية في أغلبها شركات خاصة، وأكثرها في التعليم والتجزئة والبناء والاستشارات.

الفصل 8

اقتصاد الاحتيال

يجيب هذا الفصل عن

كيف تتحول الهويات والحسابات وقنوات الدفع الإماراتية إلى أموال، وماذا أعلنت الشرطة؟

960+

حالة قبض في عملية احتيال واحدة شملت 30 دولة بقيادة وزارة الداخلية (يوليو–سبتمبر)

في هذا الفصل

8.1 تداول الحسابات المصرفية وحسابات المحافظ والدفع

8.2 بيانات البطاقات في المنشورات: رؤية ضيقة

8.3 خدمات الهوية والتحقق من هوية العميل (KYC) وشرائح SIM

8.4 الأسعار في سياقها

8.5 التحذيرات الرسمية وتحذيرات الشركات الأمنية

باختصار

أكثر خيوط الاحتيال الخاصة بالإمارات ثباتاً في بياناتنا هو سوق للحسابات الموثّقة للمقيمين: حسابات مصرفية ومحافظ رقمية وحسابات تحويل أموال وحسابات منصات تداول مرتبطة ببطاقة الهوية الإماراتية أو بطاقة الإقامة. وحوله يدور سحب أموال البطاقات عبر روابط الدفع وأجهزة نقاط البيع، وخدمات التحقق من هوية العميل (KYC)، وعمليات الاحتيال بانتحال الصفة التي حذّرت منها الشرطة طوال العام. تعاملوا مع فتح الحسابات واستعادتها كضوابط لمكافحة الاحتيال، وراقبوا التجار المستخدمين لروابط الدفع بالقدر نفسه الذي تراقبون به حاملي البطاقات.

8.1 تداول الحسابات المصرفية وحسابات المحافظ والدفع

الحسابات الإماراتية المرتبطة بهوية حقيقية هي السلعة. طلبت قنوات تجنّد من تسميهم «loaders» (أشخاص يموّلون الحسابات أو يشغّلونها لأغراض الاحتيال) حسابات تحويل ومحافظ إماراتية جديدة مرتبطة ببطاقة هوية إماراتية سارية، وذكرت حدوداً مؤكدة تبلغ 10,000 درهم (AED) (B13). وسعى منشور في يونيو إلى حسابات شركات لدى مصرفين إماراتيين، تُسلَّم «وجهاً لوجه» مع شريحة SIM وبطاقة الخصم وبطاقة الهوية الإماراتية وصلاحية الخدمات المصرفية عبر الإنترنت، لتمرير تحويلات بقيمة 50,000–150,000 USD (B14). وجنّدت منشورات في منتديات ناطقة بالروسية مشغّلين لحسابات شخصية لدى المصرفين نفسيهما (B15).

بطاقة الدليل B13 — 9 فبراير 2026

ناشر مجهول قناة تيليغرام · Telegram · الإنجليزية

النص الأصلي

```
Bring UAE [remittance app] Fresh only
with emirates id 10k AED CONFIRM
[...] guarantee
```

الترجمة

أحضروا حسابات [تطبيق تحويل أموال إماراتي] جديدة فقط مع الهوية الإماراتية بحد 10k AED مؤكد [...] ضمان

ملاحظة. جزء من سلسلة منشورات بين يناير ونوفمبر تستقطب مقيمين في الإمارات لإعارة حسابات دفع ومحافظ موثّقة.

ما يمكن إثباته

سعت قنوات التحميل (loader) إلى حسابات جديدة في تطبيق تحويل أموال إماراتي مرتبطة ببطاقة هوية إماراتية صالحة، وبحد مؤكد قدره 10,000 درهم (AED).

ما لم يثبت

لا يثبت ذلك عدد الحسابات التي قُدّمت ولا هوية أصحابها.

بطاقة الدليل B14 — 4 يونيو 2026

ناشر مجهول قناة تيليغرام · Telegram · الإنجليزية

النص الأصلي

```
Anybody have [UAE bank A] Business or
[UAE bank B] Business in Dubai [...]
50k-150k USD Work. *face to face* •
Sim Card • Debit Card • Emirates ID
(Phone number & account holder) •
Bank logs • Email
```

الترجمة

هل لدى أحد حساب أعمال لدى [مصرف إماراتي A] أو حساب أعمال لدى [مصرف إماراتي B] في دبي [...] عمل بقيمة 50k-150k USD. *وجهاً لوجه* · شريحة SIM · بطاقة خصم · الهوية الإماراتية (رقم الهاتف وصاحب الحساب) · بيانات الدخول المصرفي (Bank logs) · البريد الإلكتروني

ملاحظة. نُشر النص نفسه في قناة أخرى في 4 مايو. وسمّت إعلانات باللغة الروسية لمشغّلي الحسابات الوسيطة (drops) المصرفين نفسيهما في 22 يونيو.

ما يمكن إثباته

سعى مشترٍ إلى حسابات مصرفية تجارية إماراتية مع شريحة SIM لصاحب الحساب وبطاقة الخصم والهوية الإماراتية والوصول إلى الخدمات المصرفية عبر الإنترنت، لتحويلات بقيمة 50k-150k دولار أمريكي.

ما لم يثبت

لا يثبت ذلك تسليم أي حساب.

بطاقة الدليل B15 — 22 يونيو 2026

SOQA منتدى احتيال وبطاقات مسروقة (carding) · Forum · الروسية

النص الأصلي

```
Нужны дроповоды под физ банки [UAE bank A], [UAE bank B] UAE. Отличные условия по работе.
```

الترجمة

> مطلوب مشغّلو حسابات وسيطة (drops) لحسابات أفراد لدى [مصرف إماراتي A] و[مصرف إماراتي B]، الإمارات. ظروف عمل ممتازة.

ملاحظة. عرض إعلانان آخران (يوليو، أغسطس) حسابات وسيطة في الإمارات قادرة على تسجيل تجّار وحسابات مصرفية وحسابات في منصات الصرف.

ما يمكن إثباته	استقطب منشور باللغة الروسية في منتدى مشغّلين لحسابات أفراد وسيطة لتمرير الأموال (mule) لدى مصرفين إماراتيين مُسمَّيين.
ما لم يثبت	لا يثبت ذلك وجود حسابات وسيطة لدى هذين المصرفين أو استخدامها.

ويستهدف سحب أموال البطاقات أيضاً البنية التحتية للدفع في الإمارات. ادّعى منشور في منتدى في نوفمبر السيطرة على أجهزة دفع بحضور البطاقة في دبي، وطلب بيانات بطاقات أجنبية مسروقة (dumps، أي بيانات شرائط ممغنطة منسوخة) لتمريرها عبرها، وقال إنه يتجنب البطاقات الصادرة في الخليج (B17). وجنّدت منشورات على Telegram من تسميهم «shooters» لتمرير بطاقات مسروقة عبر روابط دفع إماراتية. وأفادت Recorded Future بأن مجموعة احتيال ناطقة بالصينية، هي Tajin، استخدمت حسابات تجار وروابط دفع بالدرهم لدى بوابات إماراتية، ورأت أنه من «المحتمل» أن المجموعة انتحلت صفة شركات إماراتية مشروعة [S34].

بطاقة الدليل B17 | 17 نوفمبر 2026

z3fraan منتدى احتيال وبطاقات مسروقة (carding) · Forum · الإنجليزية

النص الأصلي

```
i have POS in Dubai and Oman working with swiping cards "white cards" [...] i need cards or dumps from Europe and USA or Africa and worldwide no problem [...]
```

الترجمة

> لديّ أجهزة نقاط بيع (POS) في دبي وعُمان تعمل بتمرير البطاقات "البطاقات البيضاء" [...] أحتاج بطاقات أو بيانات بطاقات (dumps) من أوروبا والولايات المتحدة أو أفريقيا ومن جميع أنحاء العالم لا مشكلة [...]

ملاحظة. يقول الناشر إنه يتجنب البطاقات الصادرة في الخليج. وهذا يوجّه الخطر نحو الاستحواذ على التجّار والجهات المُصدِرة الأجنبية، لا نحو حاملي البطاقات المحليين.

ما يمكن إثباته	ادّعى مستخدم في منتدى سيطرته على أجهزة نقاط بيع تعمل بحضور البطاقة في دبي، وسعى إلى بيانات بطاقات أجنبية مسروقة (dumps) لتسييلها عبرها.
ما لم يثبت	لا يثبت ذلك وجود هذه الأجهزة ولا الجهة المستحوذة التي تخدمها.

سياق إقليمي: الاحتيال بالعملات المشفّرة. جنّد منشور منفصل في أكتوبر مزوّدي حركة مرور لأداة سحب أموال عبر موافقات العملات المشفّرة (drainer)، موجّهة على نطاق واسع إلى تجار وأفراد في الشرق الأوسط يقبلون العملات المشفّرة (B18). ولا يثبت المنشور استهداف الإمارات ولا سحب أموال البطاقات المصرفية.

بطاقة الدليل B18 | 5 أكتوبر 2026

Moon_7thShift منتدى احتيال وبطاقات مسروقة (carding)

Forum · الإنجليزية

النص الأصلي

```
We need people who know how to generate traffic for multichain approval USDT drainer [...] Traffic is needed in the direction of invoices (crypto checks), we mainly need small entrepreneurs and individuals who accept payments in cryptocurrency; rich countries of the Middle East
```

الترجمة

نحتاج أشخاصاً يعرفون كيفية توليد حركة مرور (traffic) لأداة سرقة USDT عبر الموافقات متعددة السلاسل (multichain approval drainer) [...] المطلوب حركة مرور باتجاه الفواتير (الشيكات المشفرة)، نحتاج أساساً رواد أعمال صغاراً وأفراداً يقبلون المدفوعات بالعملات المشفرة؛ الدول الغنية في الشرق الأوسط

ملاحظة. أُعيد نشره في منتدى ثانٍ في اليوم نفسه.

ما يمكن إثباته	استقطب مشغّل مزوّدي حركة مرور لأداة سرقة عملات مشفرة عبر الموافقات (approval drainer)، تستهدف تجّاراً وأفراداً في الشرق الأوسط يقبلون العملات المشفرة.
ما لم يثبت	لا يثبت ذلك وجود أي ضحايا أو خسائر في الإمارات.

8.2 بيانات البطاقات في المنشورات: رؤية ضيقة

نطاق أرقام البطاقات

تغطي هذه الأرقام فقط بطاقات الدفع التي ظهرت بنص واضح في منشورات الويب المظلم التي جُمعت لهذا التقرير. ترصد Brandefense البطاقات المسروقة بطرق أخرى كثيرة لا تشملها هذه الأرقام. وهذه الأرقام ليست مقياساً لسرقة البطاقات أو لخسائر الاحتيال.

أحصينا 631 بطاقة مختلفة مرتبطة بالإمارات ظهرت بنص واضح في المنشورات المجمّعة [S6]. نُسبت 504 منها في المنشور إلى واحدة من 14 جهة إصدار إماراتية مسمّاة، وحملت 127 وسم الدولة الإماراتي فقط. وتستحوذ أكثر جهتي إصدار تكراراً على 281 من أصل 504. يظهر أغلبها في مخرجات روبوتات فحص البطاقات في فبراير ومارس. ولأن شهري أغسطس وأكتوبر أُخذت منهما عينات ولم تُقرأ منشورات سبتمبر، فإن العدد حد أدنى. ولا ينشر التقرير إلا أعداداً على مستوى جهة الإصدار.

8.3 خدمات الهوية والتحقق من هوية العميل (KYC) وشرائح SIM

التحقق من هوية العميل ببطاقة الإقامة سوق مستقرة. عرض المشترون 5–40 USD لكل حساب في منصة عملات مشفرة أو شركة تقنية مالية جرى التحقق منه ببطاقة إقامة إماراتية (B16). وعُرضت مجموعات من صور بطاقات الهوية وجوازات السفر الإماراتية مع صور ذاتية مقابل 2.5–10 USD. وبيعت أرقام +971 افتراضية أو مسجلة عبر Telegram بنحو 1.5 USD. ترتبط هذه الخدمات مباشرة باحتيال فتح الحسابات وبالحسابات الوسيطة لتمرير الأموال (mule) الواردة في §8.1.

بطاقة الدليل B16 — 24 فبراير 2026

ناشر مجهول قناة تيليغرام · Telegram · الإنجليزية، العربية

النص الأصلي

```
Wtb [crypto exchange] United Arab Emirates [...] Price : 40$ Escrow++ You need just Residence card تحتاج فقط بطاقة الإقامة للتوثيق
```

الترجمة

مطلوب للشراء [منصة تداول عملات مشفرة] الإمارات العربية المتحدة [...] السعر: 40$ مع وسيط ضمان (Escrow++) تحتاج فقط بطاقة الإقامة

ملاحظة. كان الطلب ثابتاً على التحقق من هوية العميل (KYC) ببطاقة الإقامة الإماراتية عبر منصات التداول وتطبيقات التقنية المالية. وتراوحت الأسعار المذكورة بين 5 و40 دولاراً للحساب.

ما يمكن إثباته	عرض مشترٍ 40 دولاراً لكل حساب في منصة تداول عملات مشفرة موثّق ببطاقة إقامة إماراتية.
ما لم يثبت	لا يثبت ذلك عدد الحسابات التي اشتُريت ولا المقيمين الذين شاركوا.

بطاقة الدليل B19 — 29 أكتوبر 2026

RummRif منتدى احتيال وبطاقات مسروقة (carding) · Forum · الإنجليزية

النص الأصلي

```
750k Forex/Crypto Database From UAE For Use ●Recovery ●Depositors ●High Investors [...] Sample: Email Name Phone Country Assigned To Account Status Brand Name Original Retention Owner FTD Currency Total Deposited In USD
```

الترجمة

قاعدة بيانات فوركس/عملات مشفرة 750k من الإمارات للاستخدام في ●الاسترداد ●المودعين ●كبار المستثمرين [...] عينة: البريد الإلكتروني الاسم الهاتف الدولة مُسند إلى حالة الحساب اسم العلامة التجارية مالك الاحتفاظ الأصلي FTD العملة إجمالي الإيداع بالدولار الأمريكي

ملاحظة. تبدو أسماء الأعمدة كأنها من نظام CRM لمركز اتصال تابع لوسيط. وتُستخدم قوائم "الاسترداد" لاستهداف أشخاص خسروا أموالاً بالفعل.

ما يمكن إثباته	أدرج بائع 750,000 سجل لمودعين في الفوركس والعملات المشفرة وُصفت بأنها من الإمارات، مع مبالغ الإيداع، لاستخدامها في عمليات احتيال استرداد الأموال.
ما لم يثبت	لا يثبت ذلك الوسطاء المصدر، ولا أن المودعين يقيمون في الإمارات.

قوائم العملاء المحتملين هي مدخلات احتيال مراكز الاتصال. أدرج بائع 750,000 سجل لمودعين في منصات الفوركس والعملات المشفرة وصفها بأنها مرتبطة بالإمارات، مع مبالغ الإيداع، وصرّح بأنها مخصصة لعمليات احتيال «الاسترداد» التي تستهدف أشخاصاً خسروا أموالاً من قبل (B19).

8.4 الأسعار في سياقها

السلعة (مرتبطة بالإمارات، كما أُعلن عنها)	السعر	البطاقة
ملف عملاء شركة تأمين، 80,000 سجل	USD 200	B01
بيانات عملاء ووثائق هوية لدى شركة تطوير عقاري	USD 100	B02
صلاحية مدير أعلى على نظام ويب حكومي	USD 800	B08
مجموعة بيانات هيئة نقل، 50GB بحسب الادعاء	USD 5,000	B03
حساب منصة تداول موثّق ببطاقة إقامة إماراتية	USD 5-40	B16
مجموعة صور بطاقة هوية أو جواز سفر إماراتي مع صورة ذاتية	USD 2.5-10	لا ينطبق
رقم +971 افتراضي	نحو USD 1.5	لا ينطبق

الأسعار هي الأسعار المطلوبة في المنشورات. ولا تدل على حدوث عملية بيع أو على أصالة السلع، فالبائعون يضخّمون العروض ويعيدون تدويرها.

8.5 التحذيرات الرسمية وتحذيرات الشركات الأمنية

وصفت التحذيرات الرسمية وتحذيرات الشركات الأمنية الأنماط نفسها من جهة الضحية.

التاريخ	الجهة	ما أُعلن عنه	المصدر
2026-03-02	شرطة دبي	متصلون ينتحلون صفة موظفي إدارة الأزمات ويطلبون بيانات UAE PASS وبطاقة الهوية الإماراتية لتبديل شرائح SIM والاستيلاء على تطبيقات الخدمات المصرفية	[S49]

التاريخ	الجهة	ما أُعلن عنه	المصدر
2026-03-09	سلطة دبي للخدمات المالية (DFSA)	شركات تنتحل صفة شركات مرخّصة ونطاقات مستنسخة من السجل العام	[S53]
2026-03-10	Netcraft (شركة أمنية)	مئات الرسائل باسم "AE GOV" تحمل شعار وزارة الداخلية، أُرسلت منذ 4 مارس، روّجت لنموذج تسجيل وهمي. وطلب موقع طرود مقلِّد للجمارك رسماً قدره 20 AED	[S61]
2026-04-11	شرطة دبي	ارتفاع في المكالمات والرسائل النصية الوهمية التي تنتحل صفة مسؤولين وموظفي مصارف لطلب كلمات المرور والرموز لمرة واحدة	[S47]
2026-04-11	النيابة العامة	أرسلت شبكة رسائل نصية وهمية عن رسوم ومخالفات، بعضها بقيمة 4 AED، لجمع بيانات البطاقات. وسُجّل 35 بلاغاً، مع توقيفات منها مشتبه به محلي، وضبط 22 جهاز نقاط بيع	[S62]
2026-04-17	Unit 42 (شركة أمنية)	صفحات دفع وهمية بموضوعات بريدية، ومسارات وهمية لدفع المخالفات تنتحل صفة جهات في دبي، جمعت بيانات البطاقات	[S64]
2026-04-25	شرطة أبوظبي	حسابات وهمية على وسائل التواصل الاجتماعي تبيع تذاكر وخدمات تأشيرات ومركبات واستثمارات، وتطلب بيانات بذريعة توصيل الطرود	[S50]
2026-04-29	شرطة دبي	276 حالة قبض وتفكيك تسعة مراكز احتيال بالتعاون مع الشرطة الأمريكية والصينية	[S45]
2026-04-30	ICP (الهيئة الاتحادية للهوية والجنسية)	استُخدم اسم الهيئة وشعارها في مكالمات ومواقع للحصول على بيانات شخصية. وحذّرت الهيئة من مشاركة رموز التحقق لمرة واحدة أو رموز الهوية الرقمية	[S63]
2026-07-05	شرطة الشارقة	القبض على سبعة أشخاص انتحلوا صفة مسؤولين ودفعوا الضحايا إلى تثبيت تطبيقات منحتهم الوصول إلى هواتفهم، مع فتح حسابات مصرفية بأسماء أشخاص آخرين	[S51]
2026-07-07	شرطة دبي	مواقع وهمية لحماية المستهلك تتبعها مكالمات تدفع إلى تثبيت برامج الوصول عن بُعد أثناء استخدام الخدمات المصرفية عبر الإنترنت	[S48]
2026-10-22	وزارة الداخلية	أكثر من 960 حالة قبض وتجميد 4,126 حساباً مصرفياً في عملية شملت 30 دولة، من 1 يوليو إلى 30 سبتمبر	[S46]
2026-10-23	شرطة دبي	القبض على ستة أشخاص بسبب موقع تسوق وهمي جمع بيانات البطاقات	[S52]

قراءة مشتركة للرؤيتين. تصف المنشورات وتقارير الشرطة السلسلة نفسها: بيانات الهوية وبطاقات الإقامة تغذي فتح الحسابات، والحسابات الوسيطة تنقل الأموال، وأدوات الوصول عن بُعد والمسؤولون المزيفون يستولون على جلسات الضحايا. ويحمّل التزام المصرف المركزي برد المبالغ في حالات الاحتيال المعتمد على الرسائل النصية فقط (§10.3) جزءاً من هذه التكلفة على المؤسسات.

الخلاصات الرئيسية

01

الحسابات الإماراتية الموثّقة المرتبطة ببطاقة الهوية الإماراتية أو بطاقة الإقامة هي السلعة الأساسية في الاحتيال.

02

روابط الدفع وأجهزة الدفع بحضور البطاقة قنوات لسحب الأموال، فراقبوا التجار لا حاملي البطاقات فقط.

03

تصف تحذيرات الشرطة ومنشورات الويب المظلم السلسلة نفسها: بيانات الهوية، والحسابات الوسيطة، والاستيلاء عبر الوصول عن بُعد.

الفصل 9

نظرة معمّقة على القطاع المصرفي والمالي

يجيب هذا الفصل عن

أين يقع الانكشاف الظاهر للمصارف الإماراتية، وأي جزء منه يشير إلى اختراق لا إلى احتيال على العملاء؟

12 من 23

مصرفاً في قائمتنا لديها بيانات اعتماد مدرجة للبيع يوم الفحص

في هذا الفصل

9.1 أين يقع الانكشاف

9.2 ما تقوله المنشورات عن المصارف الإماراتية

9.3 ما غيّرته الجهة التنظيمية

9.4 ما ينبغي للمصارف فعله

باختصار

لدى جميع المصارف الـ 23 في قائمتنا أجهزة مصابة مرتبطة بنطاقاتها، لكن 98% من هذه الأجهزة تقع خارج تصنيف الموظفين، وملكيتها غير مُتحقَّق منها. وتنشر نطاقات المصارف الـ 23 كلها سياسة DMARC إنفاذية. ولدى اثني عشر مصرفاً إدراج حالي لبيانات اعتماد، وتذكر المنشورات مصارف إماراتية في تجنيد الحسابات الوسيطة وفي مخرجات فحص البطاقات. ابدأوا بفرز الإدراجات والأجهزة الـ 543 المصنفة للموظفين، ثم عزّزوا ضوابط فتح الحسابات واستعادتها.

يستخدم هذا الفصل بيانات مجمّعة فقط. المصارف الـ 23 هي المصارف المرخّصة من المصرف المركزي ضمن قائمة المؤسسات الـ 250، ومنها عمليات مصرفين أجنبيين في الإمارات ومصرف تنموي واحد. أما شركات الدفع ومنصات التداول وجهات الاستثمار فتندرج ضمن قطاع المصارف والمال الأوسع (الفصل 3).

24,526

جهازاً مصاباً مرتبطاً بنطاقات المصارف الـ 23 (543 منها مصنفة للموظفين)

71,616

سجل بيانات اعتماد: قواعد بيانات الاختراقات وسجلات برمجيات سرقة المعلومات وقوائم الدمج (combolists)

23 من 23

مصرفاً تطبّق DMARC (22 بسياسة الرفض، و 1 بسياسة الحجر)

9.1 أين يقع الانكشاف

المقياس (23 مصرفاً)	القيمة
المصارف التي لديها ارتباطات بأجهزة مصابة	23
المصارف التي لديها أجهزة مصنفة للموظفين	19
ارتباطات الأجهزة، الكل / المصنفة للموظفين	543 / 24,526
حصة الأجهزة (لا بيانات الاعتماد) لدى أكبر مصرفين	47% (71% لدى أكبر خمسة)
سجلات بيانات الاعتماد	71,616 (44,709 من قواعد بيانات الاختراقات، 7,335 من سجلات برمجيات سرقة المعلومات، 19,572 من قوائم الدمج)
المصارف التي لديها إدراج حالي لبيانات اعتماد	12

معظم الارتباطات خارج تصنيف الموظفين، وملكيتها غير مُتحقَّق منها. 23,983 من أصل 24,526 جهازاً مرتبطاً بالمصارف ليست مصنفة للموظفين. وقد يكون كثير منها أجهزة العملاء أنفسهم، لكن ملكيتها لم تثبت. وهي بالنسبة إلى المصرف مؤشر احتيال (سرقة الجلسات، والاستيلاء على الحسابات، وإساءة استخدام إجراءات الاستعادة)، ولا يمكن استبعادها مساراً للاختراق. أما الأجهزة الـ 543 المصنفة للموظفين فهي الأولوية الأولى في فرز الاختراقات.

التركّز معتدل. يحمل مصرفان ما يقارب نصف ارتباطات الأجهزة.

9.2 ما تقوله المنشورات عن المصارف الإماراتية

- **الحسابات الوسيطة لتمرير الأموال (mule).** طلبت منشورات حسابات شركات وحسابات شخصية لدى مصارف إماراتية مسمّاة مع شريحة SIM والبطاقة وبطاقة الهوية الإماراتية لصاحب الحساب (B15 ،B14)، وحسابات تحويل ومحافظ مرتبطة ببطاقة الهوية الإماراتية (B13).
- **بيانات البطاقات.** نُسبت 504 من أصل 631 بطاقة ظهرت بنص واضح في المنشورات المجمّعة إلى واحدة من 14 جهة إصدار إماراتية، وأغلبها في مخرجات فحص البطاقات في فبراير ومارس (§8.2، مع ملاحظة النطاق الخاصة به).

- **البنية التحتية لسحب الأموال.** ادّعى مستخدم في منتدى امتلاك أجهزة دفع بحضور البطاقة في دبي لسحب أموال بطاقات أجنبية (B17)، وجنّدت قنوات أشخاصاً لتمرير بطاقات مسروقة عبر روابط دفع إماراتية.
- **أسطر بيانات الاعتماد.** حملت عمليات رفع آلية أسطر تسجيل دخول إلى الخدمات المصرفية عبر الإنترنت لمصارف تجزئة إماراتية، وهي عادة تأتي من أجهزة عملاء مصابة.

9.3 ما غيّرته الجهة التنظيمية

يستهدف توجيه المصرف المركزي الصادر في مايو، ومركز عمليات مكافحة الاحتيال الذي يعتزم إنشاءه، والتزام رد المبالغ في حالات الاحتيال المعتمد على الرسائل النصية فقط (§10.3)، السلسلةَ نفسها [S36][S38]. وهي سلسلة جانب العملاء التي تصفها المنشورات. وبالنسبة إلى المصرف، باتت تكلفة أسلوب الموافقة الضعيف تقع على المصرف نفسه. ومنذ 14 سبتمبر تشمل لائحة المصرف المركزي لإدارة المخاطر التشغيلية أيضاً المؤسسات المالية المرخّصة من المصرف المركزي، وليس المصارف وحدها. وهي تشترط الإخطار خلال أربع ساعات من أي حدث له، أو يُرجَّح أن يكون له، أثر جسيم على العمليات الحيوية، وإجراء اختبارات اختراق مستقلة للوظائف الحيوية [S57].

9.4 ما ينبغي للمصارف فعله

1. **احتووا الحسابات ذات الصلاحيات المميزة وحسابات الوصول عن بُعد والحسابات غير المحمية بالمصادقة متعددة العوامل في اليوم نفسه؛ وتحقّقوا من الإدراجات الحالية الأخرى خلال خمسة أيام عمل ومن أجهزة الموظفين خلال 30 يوماً.** فهي أوضح مؤشرات الاختراق في هذا الفصل (§12.1 الصفان 2-3).
2. **تعاملوا مع ارتباطات الأجهزة الأخرى كمعلومات استخباراتية عن الاحتيال أيضاً.** أدخلوها في تقييم مخاطر الجلسات وفي المصادقة الإضافية المشددة، وصعّدوا أي ارتباط منها يتصل بموظفين أو بوصول إداري (§12.1 الصف 11).
3. **عزّزوا ضوابط فتح الحسابات ضد التحقق من هوية العميل ببطاقات الإقامة وتجنيد الحسابات الوسيطة.** اختبروها بحالات اصطناعية، وراقبوا الحسابات التي تتلقى تحويلات واردة صغيرة كثيرة وتدفعها بسرعة (§12.1 الصف 18).
4. **راقبوا التجار إلى جانب حاملي البطاقات.** روابط الدفع وأجهزة الدفع قنوات لسحب الأموال (§8.1؛ §12.1 الصف 19).

الخلاصات الرئيسية

01
معظم الأجهزة المرتبطة بالمصارف خارج تصنيف الموظفين، وملكيتها غير مُتحقَّق منها؛ افرزوا أولاً الأجهزة الـ 543 المصنفة للموظفين والإدراجات الحالية الـ 12.

02
تنشر جميع نطاقات المصارف التي قيّمناها سياسة DMARC إنفاذية؛ واصلوا اختبار مصادقة البريد الإلكتروني والحماية من التصيّد الصادر من صناديق بريد مُستولى عليها.

03
الحسابات الوسيطة، والتحقق من هوية العميل ببطاقات الإقامة، وسحب الأموال عبر روابط الدفع هي سلسلة الاحتيال التي يجب كسرها.

الفصل 10

الاستجابة التنظيمية والوطنية

يجيب هذا الفصل عن

ما القواعد والتدابير الرسمية التي تغيّرت للمؤسسات الإماراتية في 2026، وماذا ينبغي لمسؤول أمن المعلومات (CISO) أن يفعل حيالها الآن؟

4 ساعات

مهلة إخطار المؤسسات المالية المرخّصة من المصرف المركزي للمصرف المركزي بأي حدث تشغيلي جسيم، بموجب لائحة نافذة منذ 14 سبتمبر 2026

في هذا الفصل

10.1 من يضع القواعد
10.2 ما تقوله النصوص
10.3 تحوّل المصرف المركزي في المصادقة
10.4 ما فعلته الشرطة والمجلس
10.5 ما ينبغي لمسؤولي أمن المعلومات فعله الآن

باختصار

قواعد الأمن السيبراني في الإمارات متعددة المستويات: القانون الاتحادي، ومعايير على مستوى الإمارات، والأنظمة المستقلة للمنطقتين الحرتين الماليتين. وجاءت أوضح تغييرات 2026 من المصرف المركزي. أولها قاعدة إخطار بالحوادث خلال أربع ساعات للمؤسسات المالية المرخّصة من المصرف المركزي. والثاني دفع نحو تجاوز رموز التحقق لمرة واحدة عبر الرسائل النصية مع التزامات رد المبالغ في حالات الاحتيال المعتمد على الرسائل النصية فقط. حدّدوا النظام المنطبق على كل كيان، ثم تدرّبوا على الإخطار بالاختراق وفق أقصر مهلة.

هذا الفصل ليس استشارة قانونية. نذكر فقط الأحكام التي قرأناها في نص رسمي أو في مصدر ثانوي مسمّى، وحيث لم نتمكن من الحصول على نص رسمي نقول ذلك.

10.1 من يضع القواعد

المستوى	الجهة	ما تغطيه
السياسة الاتحادية	مجلس الأمن السيبراني لحكومة دولة الإمارات	الاستراتيجية الوطنية والسياسات وتنسيق الاستجابة للحوادث [S43][S54]

المستوى	الجهة	ما تغطيه
القطاع المصرفي الاتحادي	مصرف الإمارات العربية المتحدة المركزي (CBUAE)	المصارف وشركات التأمين وشركات الدفع المرخّصة [S36][S42]
البيانات والحكومة الرقمية على المستوى الاتحادي	الهيئة الاتحادية للذكاء الاصطناعي والبيانات (أُعلن عنها في 14 يونيو 2026)	الإشراف على الذكاء الاصطناعي والحكومة الرقمية وتنظيم البيانات، وفق تحليل لمكتب محاماة [S41]
الإمارة (دبي)	مركز دبي للأمن الإلكتروني (DESC)	الجهات الحكومية وشبه الحكومية في دبي [S44]
منطقة حرة مالية	مفوض حماية البيانات في مركز دبي المالي العالمي (DIFC)	الشركات في مركز دبي المالي العالمي [S39]
منطقة حرة مالية	مكتب حماية البيانات في سوق أبوظبي العالمي (ADGM)	الشركات في سوق أبوظبي العالمي [S40]

10.2 ما تقوله النصوص

الأداة التشريعية	الحكم الذي قرأناه	المصدر
قانون حماية البيانات لمركز دبي المالي العالمي رقم 5 لسنة 2020، بصيغته المعدّلة (بما في ذلك قانون التعديل رقم 1 لسنة 2025)	المادة 41: إخطار المفوض باختراق البيانات الشخصية «في أقرب وقت ممكن عملياً في ظل الظروف»؛ المادة 42: إخطار أصحاب البيانات بالاختراقات عالية المخاطر؛ الجدول 2: غرامة تصل إلى USD 50,000 عن عدم الإبلاغ بموجب أي من المادتين	[S39]
لوائح حماية البيانات لسوق أبوظبي العالمي لعام 2021	المادة 32: إخطار مكتب حماية البيانات دون تأخير غير مبرر، ومتى كان ذلك ممكناً في موعد لا يتجاوز 72 ساعة من العلم بالاختراق	[S40]
المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية	المادة 2: اختراق نظام، الحبس و/أو غرامة من 100,000 إلى 300,000 AED، وتشدَّد العقوبة عند الحصول على بيانات أو وقوع ضرر؛ المادة 3: أنظمة الجهات الحكومية، السجن المؤقت وغرامة من 200,000 إلى 500,000 AED، ولا تقل عن 5 سنوات عند وقوع ضرر أو هجوم سيبراني؛ المادة 5: الإضرار بأنظمة جهة حكومية أو منشأة حيوية، السجن المؤقت وغرامة من 500,000 إلى 3,000,000 AED، ويُعدّ ارتكابها بهجوم سيبراني ظرفاً مشدداً؛ المادة 40: الاحتيال الإلكتروني، الحبس سنة على الأقل و/أو غرامة من 250,000 إلى 1,000,000 AED. نافذ منذ 2 يناير 2022	[S56]

الأداة التشريعية	الحكم الذي قرأناه	المصدر
لائحة إدارة المخاطر التشغيلية الصادرة عن المصرف المركزي رقم C 1/2026 (نافذة منذ 14 سبتمبر 2026)	تنطبق على المؤسسات المالية المرخّصة من المصرف المركزي، وليس المصارف وحدها (تقرير صحفي عن اللائحة). إخطار المصرف المركزي خلال 4 ساعات من أي حدث له، أو يُرجَّح أن يكون له، أثر جسيم على العمليات الحيوية؛ تقرير موجز خلال 24 ساعة؛ إخطار خلال 72 ساعة عن أي حادث عالي الخطورة؛ اختبارات اختراق خارجية مستقلة للوظائف الحيوية	[S57]
مرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية (PDPL)	ساري المفعول؛ ولم تصدر لائحته التنفيذية بعد، ولم تُحدَّد بوضوح جهة إشرافية للقطاع الخاص حتى يونيو 2026، وفق تحليل لمكتب محاماة	[S41]
مرسوم بقانون اتحادي رقم (6) لسنة 2025 (قانون المصرف المركزي)	المادة 149، كما لخّصها دليل مهني: منع الاحتيال وكشفه، والإبلاغ الفوري للمصرف المركزي عن حالات الاحتيال والاختراقات الأمنية المتحقق منها	[S42]
نظام أمن المعلومات في دبي	صدر بموجب القرار رقم 13 لسنة 2012 ويُعمل به بموجب قانون دبي رقم 11 لسنة 2014، مع معايير إضافية من مركز دبي للأمن الإلكتروني لإنترنت الأشياء ومجالات أخرى	[S44]
الاستراتيجية الوطنية للأمن السيبراني	اعتمدها مجلس الوزراء في 3 فبراير 2025؛ وتقوم على خمس ركائز	[S43]

قرأنا المرسوم بقانون اتحادي رقم (34) لسنة 2021 في نص إنجليزي يستضيفه سوق أبوظبي العالمي؛ وتعذّر الوصول إلى البوابة الرسمية، ولم نتحقق من التعديلات اللاحقة. ولم نتمكن من الحصول على النص الرسمي لقانون حماية البيانات الشخصية، لذلك لا نقتبس صيغة الإخطار الواردة فيه.

10.3 تحوّل المصرف المركزي في المصادقة

تنقل المصارف الموافقة على عمليات البطاقات وتسجيل الدخول من رموز الرسائل النصية إلى تطبيقاتها. توقفت عدة مصارف كبرى عن إرسال رموز التحقق لمرة واحدة عبر الرسائل النصية لعمليات الشراء بالبطاقات عبر الإنترنت اعتباراً من 6 يناير 2026، ونقلت الموافقة إلى تطبيق المصرف [S37]. وفي 21 مايو طلب المصرف المركزي من المؤسسات المرخّصة تعزيز حماية المستهلك من الاحتيال وتقليل الاعتماد على التحقق أحادي العامل مثل رموز التحقق لمرة واحدة عبر الرسائل النصية. وأعلن أيضاً أنه بدأ إنشاء مركز مركزي لعمليات مكافحة الاحتيال لمراقبة الاحتيال في الوقت الفعلي، ولم يُنشر أي موعد نهائي [S36].

وفي يوليو، نقلت الإمارات اليوم إفصاحاً من المصرف المركزي بشأن الاحتيال المعتمد على الرسائل النصية فقط. إذ يجب على المؤسسات رد المبلغ كاملاً حين يُستخدم في الاحتيال رمز تحقق لمرة واحدة أُرسل عبر الرسائل النصية فقط، متى أبلغ العميل عنه فوراً وجرى التحقق من البلاغ [S38]. وبالنسبة إلى المصارف، ينقل ذلك تكلفة المصادقة الضعيفة إلى المؤسسة.

10.4 ما فعلته الشرطة والمجلس

استهدف إنفاذ القانون في 2026 الاحتيال على نطاق واسع. أعلنت شرطة دبي عن 276 حالة قبض وتفكيك تسعة مراكز احتيال في عملية مشتركة مع الشرطة الأمريكية والصينية أُعلن عنها في 29 أبريل [S45]. وأعلنت وزارة الداخلية عن أكثر من 960 حالة قبض وتجميد 4,126 حساباً مصرفياً في عملية شملت 30 دولة من 1 يوليو إلى 30 سبتمبر [S46]. وأصدر المجلس تنبيهات عامة، منها تحذير من برمجيات المسح التدميرية (wiper) في 4 أبريل [S11].

10.5 ما ينبغي لمسؤولي أمن المعلومات فعله الآن

1. **اربطوا كل كيان قانوني بنظامه التنظيمي.** المجموعة التي لديها شركة تابعة في مركز دبي المالي العالمي، وصندوق في سوق أبوظبي العالمي، ومصرف داخل الدولة، تواجه ثلاث قواعد للإخطار بالاختراق. احتفظوا بهذه الخريطة في خطة الاستجابة للحوادث (§12.1 الصف 12).
2. **تدرّبوا وفق أقصر مهلة.** بالنسبة إلى المؤسسات المالية المرخّصة من المصرف المركزي، أصبحت المهلة الآن أربع ساعات للإخطار [S57]. وفي غيرها، استخدموا الحد الأقصى البالغ 72 ساعة في سوق أبوظبي العالمي افتراضاً للتخطيط حيث ينطبق، و«في أقرب وقت ممكن عملياً» في مركز دبي المالي العالمي (§12.1 الصف 12).
3. **أكملوا التخلي عن رموز الرسائل النصية.** بالنسبة إلى المصارف وشركات الدفع، يجعل توجيه المصرف المركزي والتزام رد المبالغ من الموافقة عبر الرسائل النصية فقط تكلفة مباشرة [S36][S38] (§12.1 الصف 10).
4. **تابعوا اللائحة التنفيذية لقانون حماية البيانات الشخصية.** جهّزوا جرد البيانات وسجلات الاختراقات الآن، فقد تصدر القواعد التنفيذية مع الهيئة الاتحادية الجديدة [S41] (§12.1 الصف 13).

الخلاصات الرئيسية

01

تواجه المؤسسات المالية المرخّصة من المصرف المركزي الآن مهلة إخطار مدتها أربع ساعات، ولكيانات مركز دبي المالي العالمي وسوق أبوظبي العالمي قواعدها الخاصة؛ فاربطوها بكياناتكم قبل وقوع أي حادث.

02

يجعل توجيه المصرف المركزي بشأن المصادقة والتزام رد المبالغ من رموز الرسائل النصية وحدها عبئاً.

03

لا تزال قواعد حماية البيانات الاتحادية بانتظار لائحتها التنفيذية، فجهّزوا جرد البيانات الآن.

الفصل 11

التوقعات

يجيب هذا الفصل عن

ما الذي ينبغي أن تستعد له المؤسسات في الإمارات في عام 2027، وما درجة ثقتنا، وما الذي قد يغيّر الخطة؟

3

سيناريوهات مشروطة، لكلٍّ منها المؤشر الذي قد يغيّرها

في هذا الفصل

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

باختصار

تتعلق أحكامنا بالانكشاف والادعاءات، لا بنوايا الدول. يُرجَّح أن يستمر انكشاف الهوية والاحتيال على الحسابات أياً كانت التطورات الإقليمية. وقد تركّزت الادعاءات التدميرية وادعاءات ناشطي القرصنة (هاكتيفست) المرصودة في فترة التصعيد في مارس–أبريل 2026، وتغطيتنا غير مكتملة؛ فخطّطوا لتكرارها إذا عادت ظروف مماثلة. استعدّوا للأمرين معاً: واصلوا فرز الإدراجات والأجهزة على مدار العام، وأبقوا جاهزية التعافي من برمجيات المسح التدميرية (wiper) والتصدي لهجمات حجب الخدمة الموزعة (DDoS) مختبَرة استعداداً لفترة التصعيد المقبلة.

11.1 الأحكام الرئيسية

الحكم	درجة الثقة	الأساس	الحدود
سيظل انكشاف بيانات الاعتماد والأجهزة المصابة أكثر أشكال الانكشاف المقيسة شيوعاً لدى المؤسسات الإماراتية الرائدة	عالية	أعداد الفصل 3؛ وتجارة الحسابات وخدمات التحقق من هوية العميل (KYC) على مدار العام (الفصل 8)	أعداد ارتباط، لا اختراق مُتحقَّق منه
ستتركز ادعاءات ناشطي القرصنة بشأن هجمات DDoS والهجمات التدميرية حول فترات التوتر الإقليمي	متوسطة	نمط 2026: تركّزت الادعاءات في مارس–أبريل (الفصل 6)؛ والتصريحات الرسمية بشأن فترة التصعيد [S22]	بيانات عام واحد؛ وأصحاب الادعاءات يغيّرون أسماءهم؛ ولم تكن منشورات سبتمبر متاحة

الحكم	درجة الثقة	الأساس	الحدود
ستظل بيانات عملاء العقارات أكثر مجموعات البيانات الخاصة بالإمارات عرضاً؛ وستتكرر ادعاءات تخص مؤسسات منفردة في التأمين والنقل	متوسطة	حالات الفصل 4؛ وتسعة بائعين على الأقل للبيانات العقارية؛ وطلب المشترين يسبق العرض	البائعون يعيدون تدوير البيانات؛ والادعاءات غير مؤكدة
ستبقى إدراجات برامج الفدية للشركات الإماراتية أعلى بكثير من الدول الخليجية المقارَنة	متوسطة	84 إدراجاً حتى 20 نوفمبر مقابل 7–30 للدول المقارَنة [S5]	الإدراجات ادعاءات وتشمل تصنيفات خاطئة
ستدفع تغييرات مصادقة المدفوعات الاحتيالَ نحو الحسابات الوسيطة لتمرير الأموال (mule) والاستيلاء على الحسابات عبر الوصول عن بُعد وروابط الدفع	متوسطة	توجّه المصرف المركزي وواجب رد المبالغ (10.3§)؛ وتحذيرات الشرطة (8.5§)	بيانات خسائر الاحتيال غير منشورة

11.2 ما الذي قد يغيّر التقييم

- **حادثة تدميرية مؤكدة لدى جهة حكومية مسمّاة أو مشغّل حيوي** من شأنها أن تنقل تقييم المخاطر التدميرية من حكم قائم على الادعاءات إلى حكم قائم على الأدلة، وأن تبرّر استثماراً أقوى في التعافي عبر القطاعات.
- **تراجع مستدام في الإدراجات الحالية لبيانات الاعتماد** لدى المؤسسات الـ 250 عند فحص متكرر سيكون ملاحظة تحتاج إلى تفسير، لا دليلاً على نجاح الضوابط. فالإدراجات تتغيّر أيضاً مع العرض في السوق وسلوك البائعين والتغطية. والأفضل قياس الاستجابة بقرارات التصرف في الحسابات المُتحقَّق منها، وأزمنة الاستجابة، وأدلة إلغاء الجلسات، وتكرار الظهور بين الحسابات التي عولجت.
- **نشر اللوائح التنفيذية لقانون حماية البيانات الشخصية (PDPL)** سيُنشئ خط أساس للإخطار بخروقات البيانات، ويتيح مزيداً من بيانات الحوادث العامة.
- **تقرير من مورّد أو جهة رسمية يربط إدراجاً على موقع تسريب بحادثة مؤكدة في الإمارات** سيمكّننا من معايرة عدد الإدراجات التي تعكس عمليات تسلل فعلية.

11.3 سيناريوهات مشروطة

هذه افتراضات للتخطيط، وليست تنبؤات.

1. **تجدّد التوتر الإقليمي.** إذا أفادت التصريحات الرسمية مجدداً بفترة تصعيد، فتوقعوا خلال أيام ادعاءات بهجمات DDoS ضد البوابات الاتحادية والبوابات المحلية للإمارات. وتوقعوا كذلك ادعاءات اختراق وتسريب يُعاد نشرها ضد قطاعات الطاقة والموانئ والطيران، ومحاولات لاستخدام برمجيات المسح التدميرية. المؤشر: قنوات ناشطي القرصنة تنشر قوائم أهداف إماراتية.

2. **الوضع المستقر.** إذا لم تحدث فترة تصعيد، فتوقعوا أن يهيمن اقتصاد الاحتيال: تجارة الحسابات، وخدمات KYC القائمة على بطاقات الإقامة، وبيانات العملاء المحتملين في العقارات، وإدراجات برامج الفدية بوتيرة 2026. المؤشر: بقاء أسعار الإدراجات وخدمات KYC منخفضة.

3. **سدّ فجوة المصادقة.** إذا أكملت البنوك نقل الموافقة على العمليات إلى التطبيقات، فتوقعوا تحولاً نحو عمليات الاحتيال عبر الوصول عن بُعد وتسييل الأموال عبر روابط الدفع، بدلاً من سرقة رموز الرسائل النصية. المؤشر: تركيز تحذيرات الشرطة على تطبيقات الوصول عن بُعد.

الخلاصات الرئيسية

01

يُرجَّح أن يستمر انكشاف الهوية والاحتيال على الحسابات بصرف النظر عن الأحداث الإقليمية.

02

تركّزت الادعاءات التدميرية المرصودة خلال فترة التصعيد؛ خطّطوا لتكرارها إذا عادت ظروف مماثلة.

03

راقبوا الحوادث المؤكدة التي تقف وراء الإدراجات؛ فهي ستُظهر إلى أي حد تعكس الإدراجات اختراقات حقيقية.

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، لكلٍّ منها مُحفّز ومسؤول ودليل إنجاز

في هذا الفصل

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

باختصار

ابدأوا بالتأكد من أنكم تتلقّون تنبيهات إدراج بيانات الاعتماد والأجهزة المصابة، ثم تعاملوا مع ما يخصّكم تحديداً: الإدراجات الحالية، وأجهزة الموظفين، والأنظمة المكشوفة على الإنترنت. بعد ذلك، سدّوا فجوات المصادقة والبريد الإلكتروني والنسخ الاحتياطي، وتدرّبوا على سيناريوهات برمجيات المسح التدميرية وهجمات DDoS والاحتيال بالهوية، وارفعوا دليل الإنجاز لكل صف إلى مجلس الإدارة.

12.1 30/60/90 يوماً

هذا تسلسل، وليس فترة انتظار. ينبغي أن يدخل أي تهديد جوهري قائم إلى إجراءات التعامل مع الحوادث لديكم فوراً؛ ويبيّن عمود المُحفّز متى يبدأ الصف من جديد.

الصف	التوقيت	المُحفّز	الإجراء	المسؤول	دليل الإنجاز
1	الأيام 1-30	بدء الخطة	تأكّدوا من أنكم تتلقّون تنبيهات إدراج بيانات الاعتماد والأجهزة المصابة لنطاقاتكم الرئيسية؛ وإن لم يكن ذلك متاحاً، فرتّبوا له	كبير مسؤولي أمن المعلومات (CISO) واستخبارات التهديدات	تحديد مصدر التنبيه؛ واستلام أول تنبيه

الصف	التوقيت	المُحفّز	الإجراء	المسؤول	دليل الإنجاز
2	الأيام 1–30	كل تنبيه جديد بإدراج بيانات اعتماد	تحقّقوا من الحساب ومن حالة المصادقة متعددة العوامل. احتووا في اليوم نفسه الحسابات ذات الصلاحيات المميزة أو الوصول عن بُعد أو التي تفتقر إلى MFA؛ وسجّلوا قراراً بشأن البقية خلال 5 أيام عمل	فريق الهوية	لكل إدراج قرار معالجة: إعادة تعيين، أو عولج سابقاً، أو لا يخصّنا
3	الأيام 1–30	كل تنبيه جديد بجهاز موظف	تحقّقوا من ارتباطات الأجهزة المصنّفة على أنها لموظفين؛ وألغوا الجلسات والرموز المميزة حيثما كانت نشطة	فريقا الهوية والأجهزة الطرفية	مطابقة قائمة الأجهزة مع سجل الأصول؛ وتوثيق عمليات الإلغاء
4	الأيام 1–30	بدء الخطة؛ كل تحذير جديد بشأن الأنظمة الطرفية	اجردوا نقاط VPN والبريد وأنظمة CRM وCMS ومنصات تنسيق الذكاء الاصطناعي المكشوفة على الإنترنت؛ وحدّثوا الأنظمة المنتهية الدعم أو اعزلوها؛ وافرضوا تسجيل الدخول الموحّد والمصادقة متعددة العوامل على منصات إدارة المحتوى وواجهات الإدارة، وأزيلوا حسابات المدير المحلية	البنية التحتية	نجاح إعادة الاختبار الخارجي؛ واعتماد الاستثناءات
5	الأيام 1–30	بدء الخطة؛ كل تحذير جديد بشأن الكاميرات	حدّثوا كاميرات IP وأجهزة التسجيل أو أزيلوا انكشافها على الإنترنت، بما في ذلك CVE-2017-7921 وCVE-2021-33044، وفق البرامج الثابتة المتأثرة والمُصلَحة بحسب الطراز في §7.2	المرافق والبنية التحتية	جرد الكاميرات؛ وإعادة اختبار خارجي لا تُظهر واجهات إدارة مكشوفة
6	الأيام 1–30	بدء الخطة؛ كل تحذير من برمجيات المسح التدميرية	استعيدوا نظاماً حيوياً من نسخة احتياطية غير متصلة خلال زمن الاستعادة المتعهَّد به	البنية التحتية واستمرارية الأعمال	سجل استعادة موقوت

الصف	التوقيت	المُحفّز	الإجراء	المسؤول	دليل الإنجاز
7	الأيام 31-60	بدء الخطة	فعّلوا التنبيه عند ظهور أدوات إدارة عن بُعد جديدة، وعند التحميل الجانبي لملفات DLL من مسارات قابلة للكتابة من قِبل المستخدم، وعند الاتصالات الصادرة غير المعتادة من خوادم CRM والبريد	مركز العمليات الأمنية (SOC)	الكشف مفعّل؛ وإطلاق تنبيه اختباري
8	الأيام 31-60	بدء الخطة	افرضوا سياسة DMARC بوضع الرفض (reject) أو العزل (quarantine) على كل نطاق إرسال	مالكو البريد الإلكتروني وDNS	سياسة DMARC لكل نطاق
9	الأيام 31-60	بدء الخطة؛ والتجديد عندما يعلن المجلس أو الشرطة فترة تصعيد	تعاقدوا على خدمات التخفيف من هجمات DDoS لدى مزوّد المنبع للبوابات العامة	البنية التحتية والشبكات	عقد التخفيف قائم؛ واختبار التحويل الاحتياطي
10	الأيام 31-60	بدء الخطة	انقلوا ما تبقّى من موافقات العملاء والموظفين بعيداً عن الرموز لمرة واحدة عبر الرسائل النصية	القنوات الرقمية ومكافحة الاحتيال	نسبة الموافقات حسب الطريقة، قبل وبعد
11	الأيام 31-60	كل تنبيه جديد بجهاز عميل (المصارف وشركات الدفع)	أدخلوا ارتباطات الأجهزة غير المصنفة للموظفين في تقييم مخاطر الجلسات والمصادقة الإضافية المشددة	مكافحة الاحتيال والقنوات الرقمية	المؤشر مفعّل في تقييم المخاطر؛ وإجراء أول مراجعة
12	الأيام 31-60	بدء الخطة؛ أي كيان قانوني أو قاعدة جديدة	اربطوا كل كيان قانوني بنظام الإخطار المنطبق عليه (قاعدة الساعات الأربع للمصرف المركزي، وداخل الدولة onshore، وDIFC، وADGM)، وتدرّبوا وفق أقصر مهلة	الشؤون القانونية والخصوصية	خريطة ضمن خطة الاستجابة للحوادث؛ وتوقيتات التمرين

الصف	التوقيت	المُحفّز	الإجراء	المسؤول	دليل الإنجاز
13	الأيام 31-60	بدء الخطة؛ والتحديث عند صدور اللائحة التنفيذية لقانون حماية البيانات الشخصية	جهّزوا جرد البيانات وسجلات الاختراقات؛ وحدّثوا خريطة الإخطار	الخصوصية	الجرد وسجل الاختراقات قائمان؛ وتحديث الخريطة
14	الأيام 31-60	بدء الخطة؛ كل ادعاء جديد ببيع بيانات يذكركم	راجعوا عمليات التصدير من منصات CRM وبرامج الولاء، ووصول الشركاء	مالكو البيانات	اعتماد مراجعة سجل التصدير
15	الأيام 61-90، أو فوراً عند وقوع المحفّز	ادعاء بيع بيانات أو تسريبها يذكر عملاءكم، بعد تقييم عيّنة أو قائمة حقول على أنها ذات مصداقية، أو حادثة مؤكدة	حذّروا العملاء من انتحال الهوية باستخدام بيانات مسرّبة عن العقارات أو وثائق التأمين أو برامج الولاء، في إشعار توعوي لا يؤكد وقوع اختراق	اتصالات العملاء	نشر الإشعار
16	الأيام 61-90	بدء الخطة؛ كل ادعاء يذكركم	تدرّبوا على سيناريو هجوم DDoS وادعاء تسريب من ناشطي القرصنة، بما في ذلك تحديد من يؤكد الوضع علناً؛ وتحقّقوا من كل ادعاء فعلي مقابل بيانات الرصد ومع مالك النظام	الاتصال المؤسسي وSOC	تقرير التمرين مع التوقيتات
17	الأيام 61-90	بدء الخطة؛ كل تحذير من برمجيات المسح التدميرية	تدرّبوا على سيناريو برمجيات المسح التدميرية عبر بيئتي تقنية المعلومات (IT) والتقنيات التشغيلية (OT)	CISO ومالكو أنظمة OT	تقرير التمرين؛ وإسناد الفجوات إلى مسؤولين
18	الأيام 61-90	بدء الخطة؛ نمط جديد للتحقق من الهوية أو تبديل شرائح SIM في التحذيرات	اختبروا إجراءات فتح الحسابات واستعادتها في مواجهة احتيال بطاقات الإقامة وتبديل شرائح SIM باستخدام حالات اصطناعية؛ وتشدّد شركات الاتصالات ضوابط تبديل الشرائح ونقل الأرقام	مكافحة الاحتيال والهوية	نتائج الاختبار؛ وتعديل الضوابط

الصف	التوقيت	المُحفّز	الإجراء	المسؤول	دليل الإنجاز
19	الأيام 61-90	بدء الخطة	راقبوا التجار وروابط الدفع لرصد أنماط تسييل الأموال	خدمات قبول المدفوعات ومكافحة الاحتيال	تفعيل القواعد؛ وإجراء أول مراجعة
20	الأيام 61-90	اليوم 90، ثم كل ربع سنة	أبلغوا عن قرارات التصرف في الحسابات المُتحقَّق منها، وأزمنة الاستجابة، وإلغاء الجلسات، وتكرار الظهور بين الحسابات التي عولجت؛ واعرضوا أعداد الإدراجات والأجهزة سياقاً فقط	CISO	ورقة لمجلس الإدارة تعرض مقاييس الاستجابة وسياق ما قبل وما بعد

12.2 حسب الدور

- **مجالس الإدارة والتنفيذيون.** اطلبوا معدّل البتّ في الإدراجات وزمن الاستعادة الموقوت من النسخ الاحتياطية. يمكن قياس كليهما خلال 30 يوماً.
- **كبار مسؤولي أمن المعلومات.** تعاملوا مع أي إدراج حالي لبيانات الاعتماد بوصفه محفّزاً لإجراءات الحوادث. وموّلوا التعافي من برمجيات المسح التدميرية والتخفيف من هجمات DDoS على مستوى مزوّد الخدمة قبل فترة التصعيد المقبلة.
- **مراكز العمليات الأمنية واستخبارات التهديدات.** ابحثوا استباقياً عن ملفات DLL المحمّلة جانبياً وأدوات الإدارة عن بُعد وحركة الخروج غير المعتادة من خوادم البريد وCRM. وتحقّقوا من كل ادعاء لناشطي القرصنة مقابل بيانات القياس عن بُعد قبل رفعه إلى مستوى أعلى.
- **فرق مكافحة الاحتيال.** ركّزوا على فتح الحسابات واستعادتها، والحسابات الوسيطة لتمرير الأموال (mule)، وروابط الدفع. لم تعد رموز الرسائل النصية عاملاً منفرداً يمكن الدفاع عنه.
- **الاتصال المؤسسي والشؤون القانونية.** أعدّوا بيانات مؤقتة للتعامل مع الادعاءات غير المؤكدة، وأبقوا خريطة الإخطار محدّثة.

12.3 كيف يمكن أن تساعد Brandefense

تجمع Brandefense بين استخبارات التهديدات السيبرانية (Cyber Threat Intelligence) وحماية المخاطر الرقمية (Digital Risk Protection) وإدارة سطح الهجوم الخارجي (External Attack Surface Management). استخدم التحليل الوارد في هذا التقرير البيانات وآلية التقييم نفسيهما اللتين تطبّقهما المنصة على المؤسسات الخاضعة للمراقبة. وتشمل هذه البيانات ارتباطات الأجهزة المصابة وبيانات الاعتماد، والإدراجات الحالية في أسواق بيانات الاعتماد، والنطاقات المشابهة، والمستندات المكشوفة، والإشارات على الويب المظلم. ولا يَعِد التحليل بإمكانية التحقق من كل ادعاء، ولا بأن السجل التاريخي يظل قابلاً للاستخدام.

احضروا نطاقاتكم وعلاماتكم التجارية وأولوياتكم الأمنية إلى عرض توضيحي مدته 30-45 دقيقة مع فريقي المبيعات وما قبل البيع. يمكن للفريق أن يوضح كيف تربط مراقبة المنصة الإشارات الخارجية بالأصول التي تديرونها. وسيتواصل معكم أحد أعضاء فريق Brandefense أو شريك في منطقتكم.

اطلب عرضاً توضيحياً

الخلاصات الرئيسية

01

ابدأوا بالتنبيهات والإدراجات وأجهزة الموظفين؛ فهي محددة وقابلة للقياس.

02

اختبروا استعادة النسخ الاحتياطية والجاهزية لهجمات DDoS قبل فترة التصعيد المقبلة.

03

قيسوا التقدّم بأدلة الإنجاز، لا بالخطط.

الملحق A. المنهجية

A.1 النطاق الزمني والمصادر والأولوية

فترة البحث هي 1 يناير–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، وبيانات البطاقات الواردة في المنشورات)، وRansompedia (إدراجات مواقع تسريب برامج الفدية)، وتقييمات الانكشاف في Brandefense Atlas. توفّر المصادر الخارجية السياق، ولا يُستشهد بها إلا بعد قراءة المقطع الداعم. استُخرجت البيانات في 21 نوفمبر 2026. المصادر S1–S6 هي بيانات Brandefense الخاصة وليس لها عنوان عام؛ وكل مصدر خارجي في الملحق C مرفق برابط وبتاريخ التحقق منه.

A.2 منشورات Blackhole

البند	القيمة
المنشورات التي تحمل وسم دولة الإمارات	130,477 منشوراً معدوداً
التغطية	نطاقات المنشورات ذات الصلة لأشهر يناير–يوليو ونوفمبر؛ وتغطية جزئية لأغسطس وأكتوبر؛ ومنشورات سبتمبر غير متاحة
منشورات المنتديات	منشورات المنتديات التي تذكر الإمارات؛ 1,271 منشوراً مميزاً

البند	القيمة
المنشورات ذات الصلة (بعد التنقية)، يناير-يوليو ونوفمبر	23,663-24,456 من أصل 65,544، تُعرض نطاقاً

من بين 30 منشوراً عشوائياً ذا صلة، كان 27 مرتبطاً بالجريمة، وذكر 10 الإمارات تحديداً. لذا تمثّل الأعداد بعد التنقية حداً أعلى للنشاط الإجرامي الخاص بالإمارات.

يحدّد قيدان كل اتجاه في هذا التقرير. لا نقارن أعداد العائلات عبر يونيو 2026. ولم تكن منشورات سبتمبر متاحة؛ ولا يظهر سبتمبر إلا في الأعداد الشهرية وفي منشورات المنتديات التي تذكر الإمارات.

A.3 المؤسسات الـ 250

ترد معايير الاختيار والتحقق والحدود في §3.1. قرأنا لكل نطاق رئيسي إشارات الانكشاف التي يستخدمها Atlas في تقييماته. وهي الأجهزة المصابة، وأجهزة الموظفين، وسجلات بيانات الاعتماد، والإشارات في المحادثات المظلمة والويب المظلم، والنطاقات المشابهة الجديدة، والمستندات التي تشير إلى النطاق، والإدراجات الحالية والسابقة في أسواق بيانات الاعتماد. قُرئت البيانات في 21 نوفمبر 2026.

A.4 تقييمات Atlas

حصلت كل مؤسسة على تقييم انكشاف من Atlas بناءً على هذه الإشارات. ويُعرض الرقم الرئيسي الوطني كما يعطيه Atlas، وتُعرض نتائج القطاعات أعداداً للإشارات. تعاملوا مع الإدراج الحالي في سوق بيانات الاعتماد على أنه سبب للتحقق من الحسابات، لا دليل على حدوث اختراق.

كانت لدى 205 مؤسسات مطابقات مرشّحة لنطاقات شبيهة؛ ولم يُتحقَّق من جميع هذه المطابقات.

A.5 فحوص DNS وTLS والويب

فحصنا سجلات DNS العامة الخاصة بالبريد ومصادقة البريد الإلكتروني وDNSSEC، كما فحصنا TLS والصفحة الرئيسية لكل نطاق. تُحتسب سياسات DMARC المفقودة وغير الصالحة وسياسات المراقبة فقط (p=none) على أنها غياب للإنفاذ. لم يتجاوز أي فحص هذه الفحوص السلبية. مؤشر سلامة الإعدادات السلبي (passive hygiene index) مؤشر تحليلي مركّب من Odin يجمع هذه الفحوص على مقياس من 0-100؛ وتعني القيمة الأعلى سلامة أضعف. وهو نموذج، وليس تقييماً من Atlas. وقيمة القطاع هي ملخّص المؤشر لذلك القطاع، وليست متوسطاً لمؤسساته.

A.6 بيانات البطاقات في المنشورات

النطاق: بطاقات الدفع التي ظهرت كنص واضح في منشورات الويب المظلم المجمّعة لهذا التقرير فقط. ترصد Brandefense البطاقات المسروقة عبر أساليب أخرى كثيرة تقع خارج نطاق هذا التقرير. لا تقيس هذه الأرقام سرقة البطاقات ولا خسائر الاحتيال. ولا ينشر التقرير إلا أعداداً على مستوى الجهة المُصدِرة.

A.7 برامج الفدية

استخدمنا الإدراجات المقبولة في Ransompedia للإمارات والسعودية وقطر والكويت وعُمان، لجميع التواريخ، مؤرَّخة بتاريخ النشر. واستُبعدت الإدراجات المرفوضة والمكررة. ولا يُستخدم متتبّع عام ومنشورات Blackhole المُعاد نشرها إلا للتحقق المتقاطع.

A.8 تغطية الحوادث

تجمع تغطية الحوادث بين بيانات منشوراتنا عن المؤسسات الـ 250، والتقارير العامة بالإنجليزية والعربية والروسية، والصفحات الرسمية الإماراتية طوال فترة البحث، مع فحص أخير حتى 20 نوفمبر 2026.

حدود التغطية المتبقية. رؤيتنا جزئية:

- لم تكن التقارير العامة بالعمق نفسه لكل مؤسسة.
- اعتمدنا في بعض النصوص الرسمية، ومنها التشريعات الاتحادية ودليل قواعد المصرف المركزي، على نسخ مستضافة في مواقع أخرى أو على مصادر ثانوية مسمّاة، كما هو موضّح في الإحالات.
- لا تُغطّى مواقع تسريب برامج الفدية على شبكة Tor إلا من خلال Ransompedia.
- تقع المنتديات المغلقة والمجموعات الخاصة وعمليات البيع المرتّبة عبر الرسائل المباشرة خارج نطاق جمعنا.
- تبقى الحوادث التي تعالجها المؤسسات دون إفصاح غير مرئية.

إن غياب حادثة عن هذا التقرير لا يعني أنها لم تقع.

A.9 الثقة والحدود

تنطبق الثقة العالية على قياس قابل للتكرار، لا على الادعاء الأصلي الصادر عن مجرم. وتشير الثقة المتوسطة إلى تفسير يستند إلى سند داعم واضح مع حدود مُعلنة. وتعني عبارة "غير مؤكد" أن الأمر لم يُثبت بشكل مستقل؛ وهي ليست دليلاً على التلفيق ولا دليلاً على وقوع اختراق. تُوصف المؤسسات الضحية بحسب دورها، ولا تُسمّى جهة أو شركة إلا حيث أُكّدت الحادثة رسمياً ونُشرت على نطاق واسع. ولا تُنقل الإسنادات إلى دول إلا كما يذكرها المصدر، ولا يُجري المؤلفون أي إسناد من عندهم. تُذكر الأسماء المستعارة للجهات الفاعلة، وتُحجب الروابط وبيانات الاتصال والمؤشرات والبيانات الشخصية.

الملحق B. سجل الأدلة

يظهر كل منشور مقتبس في هذا التقرير على شكل بطاقة منشور منقّحة في الفصل المبيّن. المقتطفات قصيرة، وتُعلَّم المحذوفات بـ [...]. وتُستبدل المعرّفات وبيانات الاتصال والروابط والمؤسسات الضحية بتسميات بين أقواس معقوفة، وفق السياسة الواردة في A.9. وتُستبعد التصريحات السياسية والدينية الواردة في منشورات الجهات الفاعلة. الترجمات من إعدادنا ما لم يتضمن المنشور نص الجهة الفاعلة نفسها بالإنجليزية. تواريخ النشر ليست تواريخ التسلل.

البطاقة	تاريخ النشر	المنصة	الاسم المستعار كما يظهر	اللغة	يظهر في
B01	2026-01-30	منتدى تسريبات	بائع بيانات شركة التأمين (الاسم المستعار محجوب)	الإنجليزية	4.6§
B02	2026-04-02	منتدى تسريبات	بائع البطاقة B01 (الاسم المستعار محجوب)	الإنجليزية	4.4§
B03	2026-11-15	منتدى تسريبات	databreach000	الإنجليزية	4.6§
B04	2026-04-13	منتدى تسريبات	ksa901	الإنجليزية	4.4§
B05	2026-09-10	منتدى لتجميع التسريبات	حساب تجميعي (معرّف الجهة الفاعلة محجوب)	الإنجليزية	6.3§
B06	2026-05-06	منتدى تسريبات	attackercompany	الإنجليزية	4.4§
B07	2026-01-26	منتدى تسريبات	Retrogade	الإنجليزية	4.5§
B08	2026-04-26	منتدى تسريبات	Crimson	الإنجليزية	4.5§
B09	2026-03-23	منتدى تسريبات	rSosa	الإنجليزية	4.5§
B10	2026-02-24	منتدى تسريبات	TheAshborn	الإنجليزية	4.5§
B11	2026-03-05	منتدى تسريبات	CVDEAD	الإنجليزية	4.5§

البطاقة	تاريخ النشر	المنصة	الاسم المستعار كما يظهر	اللغة	يظهر في
B12	2026-08-11	منتدى لتجميع التسريبات	روبوت X Forum	الإنجليزية	4.5§
B13	2026-02-09	قناة Telegram	ناشر مجهول	الإنجليزية	8.1§
B14	2026-06-04	قناة Telegram	ناشر مجهول	الإنجليزية	8.1§
B15	2026-06-22	منتدى بطاقات/احتيال	SOQA	الروسية	8.1§
B16	2026-02-24	قناة Telegram	ناشر مجهول	الإنجليزية، العربية	8.3§
B17	2026-11-17	منتدى بطاقات/احتيال	z3fraan	الإنجليزية	8.1§
B18	2026-10-05	منتدى بطاقات/احتيال	Moon_7thShift	الإنجليزية	8.1§
B19	2026-10-29	منتدى بطاقات/احتيال	RummRif	الإنجليزية	8.3§
B20	2026-02-18	منتدى تسريبات	مشترٍ مجهول	الإنجليزية	4.4§
B21	2026-03-02	قناة الجهة الفاعلة	Team 313	العربية، الإنجليزية	6.2§
B22	2026-03-12	قناة الجهة الفاعلة	+Keymous	الإنجليزية	6.2§
B23	2026-03-27	منتدى تسريبات	coderx	الإنجليزية	6.3§
B24	2026-06-01	قناة الجهة الفاعلة	Golden Falcon	الإنجليزية	6.3§

الملحق C. المصادر

S1 مجموعة منشورات Brandefense Blackhole، وسم دولة الإمارات ومنشورات المنتديات التي تذكر الإمارات، تواريخ النشر 1 يناير–20 نوفمبر 2026، استُخرجت في 21 نوفمبر 2026.

S2 ارتباطات Brandefense Blackhole بالأجهزة المصابة وقواعد بيانات الخروقات وسجلات برمجيات سرقة المعلومات وقوائم combolist لـ 250 نطاقاً، قُرئت في 21 نوفمبر 2026.

S3 تقييمات الانكشاف من Brandefense Atlas للنطاقات الـ 250، 21 نوفمبر 2026، وتشمل إدراجات أسواق بيانات الاعتماد والنطاقات المشابهة والمستندات المكشوفة والإشارات.

S4 فحوص Brandefense العامة لـ DNS وTLS والصفحة الرئيسية للنطاقات الـ 250، 21 نوفمبر 2026.

S5 Brandefense Ransompedia، الإدراجات المقبولة للإمارات والسعودية وقطر والكويت وعُمان، جميع التواريخ، استُخرجت في 21 نوفمبر 2026.

S6 استخراج Brandefense Blackhole للبطاقات المرتبطة بالإمارات التي ظهرت كنص واضح في المنشورات المجمّعة، 21 نوفمبر 2026.

S7 ransomware.live، ضحايا الإمارات حسب الدولة، تم الاطلاع في 21 نوفمبر 2026 (للتحقق المتقاطع فقط). https://www.ransomware.live/ (رابط المقال محجوب). تم التحقق في 21 نوفمبر 2026.

S8 DataReportal، "Digital 2026: the United Arab Emirates". https://datareportal.com/reports/digital-2026-united-arab-emirates. تم التحقق في 21 نوفمبر 2026.

S9 Khaleej Times (WAM)، "Over 70% of cyber threats targeting UAE are state-sponsored, authority says"، 18 فبراير 2026. https://www.khaleejtimes.com/uae/over-70-of-cyber-threats-targeting-uae-are-state-sponsored-authority-says. تم التحقق في 21 نوفمبر 2026.

S10 The National، "UAE foils AI-powered 'terrorist cyber attacks' on vital sectors"، 22 فبراير 2026. https://www.thenationalnews.com/news/uae/2026/02/22/uae-foils-ai-powered-terrorist-cyberattacks-on-vital-sectors. تم التحقق في 21 نوفمبر 2026.

S11 مجلس الأمن السيبراني لحكومة دولة الإمارات، نشرة تحذيرية "Wiper Malware Campaign Targeting Multiple Sectors"، 4 أبريل 2026 (TLP:WHITE)، مستضافة لدى ADGM. https://assets.adgm.com/download/assets/432318719+-+Wiper+Malware+Campaign+Targeting+Multiple+Sectors.pdf/af059afe318811f1b18b0634db0fb850. تم التحقق في 21 نوفمبر 2026.

S12 Gulf News، "UAE Cyber Security Council warns against wiper malware threat"، حُدّث في 19 مارس 2026. https://gulfnews.com/uae/uae-cyber-security-council-warns-against-wiper-malware-threat-1.500480274. تم التحقق في 21 نوفمبر 2026.

S13 Khaleej Times، تقرير عن تصريحات رئيس مجلس الأمن السيبراني لحكومة دولة الإمارات في قمة SAMENA 1، أبريل 2026. https://www.khaleejtimes.com/business/uae-cyberattacks-triple-to-600000-amid-iran-conflict-says-cybersecurity-chief. تم التحقق في 21 نوفمبر 2026.

S14 الإمارات اليوم، تقرير عن تصريحات رئيس مجلس الأمن السيبراني لحكومة دولة الإمارات في الفجيرة (بالعربية)، 20 أبريل 2026. https://www.emaratalyoum.com/local-section/other/2026-04-20-1.2037698. تم التحقق في 21 نوفمبر 2026.

S15 Khaleej Times (WAM)، "UAE authority foils sophisticated cyberattacks on entities in financial sector"، 3 يوليو 2026. https://www.khaleejtimes.com/uae/foils-cyberattacks-entities-financial-sector. تم التحقق في 21 نوفمبر 2026.

S16 Gulf News (WAM)، "UAE foils advanced cyberattacks targeting vital sectors"، 10 أغسطس 2026. https://gulfnews.com/amp/story/uae%2Fuae-foils-advanced-cyberattacks-targeting-vital-sectors-1.500636064. تم التحقق في 21 نوفمبر 2026.

S17 Khaleej Times، "$5 million ransom: UAE official recalls how country responded to major cyberattack"، 15 سبتمبر 2026 (حُدّث في 16 سبتمبر). https://www.khaleejtimes.com/uae/records-640000-cyberattacks-a-day-chief-reveals. تم التحقق في 21 نوفمبر 2026.

S18 The National، تقرير عن مقابلة أجرتها CNN مع رئيس مجلس الأمن السيبراني لحكومة دولة الإمارات، 16 سبتمبر 2026. https://www.thenationalnews.com/news/uae/2026/09/16/irans-irgc-behind-many-cyberattacks-on-uae-says-security-chief/. تم التحقق في 21 نوفمبر 2026.

S19 Euronews، مقابلة مع رئيس مجلس الأمن السيبراني لحكومة دولة الإمارات في قمة الإعلام العربي، 17 سبتمبر 2026. https://www.euronews.com/2026/09/17/every-iranian-strike-came-with-a-cyberattack-uae-cyber-chief-says. تم التحقق في 21 نوفمبر 2026.

S20 Khaleej Times (WAM)، "UAE foils around 750,000 cyberattacks targeting sectors including energy, education"، 21 أكتوبر 2026. https://www.khaleejtimes.com/uae/thwarts-750000-cyberattack-attempts. تم التحقق في 21 نوفمبر 2026.

S21 الإمارات اليوم، تقرير عن تصريحات رئيس مجلس الأمن السيبراني لحكومة دولة الإمارات خلال أسبوع الأمن السيبراني لبلدية دبي (بالعربية)، 28 أكتوبر 2026. https://www.emaratalyoum.com/local-section/other/2026-10-28-1.2096890. تم التحقق في 21 نوفمبر 2026.

S22 Khaleej Times، "Over 40 cyber groups tried to attack UAE infrastructure amid regional crisis, official says"، 18 نوفمبر 2026. https://www.khaleejtimes.com/uae/over-40-cyber-groups-tried-to-attack-uae-infrastructure-amid-regional-crisis-official-says. تم التحقق في 21 نوفمبر 2026.

S23 الإمارات اليوم، تقرير عن تصريحات رئيس مجلس الأمن السيبراني لحكومة دولة الإمارات في القمة العالمية للشرطة (بالعربية)، 19 نوفمبر 2026. https://emaratalyoum.com/local-section/accidents/2026-11-19-1.2104340. تم التحقق في 21 نوفمبر 2026.

S24 The National، "UAE's Landmark Group probes data breach in Shukran loyalty programme"، 11 نوفمبر 2026. https://www.thenationalnews.com/business/money/2026/11/11/uaes-landmark-group-probes-data-breach-for-its-shukran-loyalty-programme/. تم التحقق في 21 نوفمبر 2026.

S25 Khaleej Times، "Shukran members' personal data accessed in data breach, but card details safe"، 11 نوفمبر 2026. https://www.khaleejtimes.com/business/shukran-members-personal-data-accessed-in-data-breach-but-card-details-safe. تم التحقق في 21 نوفمبر 2026.

S26 Security Affairs، "Iran-linked group Handala claims to have breached three major UAE organizations"، 13 أبريل 2026. https://securityaffairs.com/190716/hacking/iran-linked-group-handala-claims-to-have-breached-three-major-uae-organizations.html. تم التحقق في 21 نوفمبر 2026.

S27 صفحة أخبار UpGuard بشأن ادعاء ضد مشغّل موانئ إماراتي، مايو 2026. https://www.upguard.com/ (رابط المقال محجوب). تم التحقق في 21 نوفمبر 2026.

S28 Daily Dark Web، تقرير عن ادعاء مزعوم ضد مشغّل مطار إماراتي، 31 مارس 2026. https://dailydarkweb.net/ (رابط المقال محجوب). تم التحقق في 21 نوفمبر 2026.

S29 The National، "Missile attacks and cyber hacks: Dual threats of modern warfare"، 2 مارس 2026. https://www.thenationalnews.com/future/technology/2026/03/02/cyberwar-and-military-escalation-converge-as-middle-east-digital-infrastructure-is-attacked. تم التحقق في 21 نوفمبر 2026.

S30 StormWall، "DDoS Threat Landscape in MENA: Q1 2026 Report" (صفحة غير مؤرّخة). https://stormwall.network/resources/blog/q1-2026-ddos-report-mena. تم التحقق في 21 نوفمبر 2026.

S31 Palo Alto Networks Unit 42، "Boggy Serpens threat assessment"، 16 مارس 2026. https://unit42.paloaltonetworks.com/boggy-serpens-threat-assessment/. تم التحقق في 21 نوفمبر 2026.

S32 Palo Alto Networks Unit 42، "Tracking Iranian APT Screening Serpens' 2026 Espionage Campaigns"، 22 مايو 2026. https://unit42.paloaltonetworks.com/tracking-iran-apt-screening-serpens/. تم التحقق في 21 نوفمبر 2026.

S33 ESET، "ESET APT Activity Report Q4 2025-Q1 2026"، 28 مايو 2026. https://www.welivesecurity.com/en/eset-research/eset-apt-activity-report-q4-2025-q1-2026/. تم التحقق في 21 نوفمبر 2026.

S34 Recorded Future Insikt Group، "Inside Tajin Group's Phishing and Money Laundering Network" (صفحة غير مؤرّخة؛ بيانات حتى يوليو 2026). https://www.recordedfuture.com/research/tajin-group-gurantee-marketplace. تم التحقق في 21 نوفمبر 2026.

S35 Khaleej Times، "91% of UAE DDoS attacks are low-volume as threats turn stealthier"، 22 سبتمبر 2026 (بيانات Help AG). https://www.khaleejtimes.com/business/91-of-uae-ddos-attacks-are-low-volume-as-threats-turn-stealthier. تم التحقق في 21 نوفمبر 2026.

S36 Gulf News، "UAE banks ordered to tighten anti-fraud security beyond OTPs"، 21 مايو 2026. https://gulfnews.com/business/banking/uae-banks-ordered-to-tighten-anti-fraud-security-beyond-otps-1.500548327. تم التحقق في 21 نوفمبر 2026.

S37 Gulf News، "UAE banks to end SMS OTPs for online card payments from January 6"، حُدّث في 2 يناير 2026. https://gulfnews.com/business/banking/uae-banks-to-end-sms-otps-for-online-card-payments-from-january-6-1.500396452. تم التحقق في 21 نوفمبر 2026.

S38 الإمارات اليوم، تقرير عن إفصاح من المصرف المركزي بشأن رد مبالغ الاحتيال في العمليات المعتمدة على الرسائل النصية وحدها (بالعربية)، 16 يوليو 2026. https://www.emaratalyoum.com/business/local/2026-07-16-1.2065407. تم التحقق في 21 نوفمبر 2026.

S39 DIFC، Data Protection Law, DIFC Law No. 5 of 2020، بصيغته المعدّلة (بما في ذلك DIFC Laws Amendment Law (No. 1 of 2025). https://www.difc.com/business/laws-and-regulations/legal-database/difc-laws/data-protection-law-difc-law-no-5-2020. قانون التعديل: https://assets.difc.com/v1/media/edge/images/dubaiintern0078-difcexperie96c5-production-3253/media/project/difcexperiences/difc/difcwebsite/documents/laws--regulations/amendment-law-no-1-of-2025.pdf. تم التحقق في 21 نوفمبر 2026.

S40 ADGM Office of Data Protection، "Personal Data Breach Notifications". https://www.adgm.com/operating-in-adgm/office-of-data-protection/data-breach-notifications. تم التحقق في 21 نوفمبر 2026.

S41 Morgan Lewis، "UAE establishes Federal Authority for Artificial Intelligence and Data"، يونيو 2026. https://www.morganlewis.com/pubs/2026/06/uae-establishes-federal-authority-for-artificial-intelligence-and-data. تم التحقق في 21 نوفمبر 2026.

S42 Chambers and Partners، "Cybersecurity 2026: UAE, trends and developments" (من تأليف فريق Ankura؛ غير مؤرّخ). https://chambers.com/practice-guides/guides/cybersecurity-2026/uae/trends-and-developments. تم التحقق في 21 نوفمبر 2026.

S43 المكتب الإعلامي لحكومة دبي، اجتماع مجلس الوزراء الإماراتي الذي اعتمد الاستراتيجية الوطنية للأمن السيبراني، 3 فبراير 2025. https://mediaoffice.ae/en/news/2025/february/03-02/mohammed-bin-rashid-chairs-cabinet-meeting. تم التحقق في 21 نوفمبر 2026.

S44 مركز دبي للأمن الإلكتروني، "Standards and policies". https://www.desc.gov.ae/regulations/standards-policies/. تم التحقق في 21 نوفمبر 2026.

S45 The National، "Almost 300 arrested in joint UAE, US, Chinese crackdown on financial crime"، 29 أبريل 2026. https://www.thenationalnews.com/news/uae/2026/04/29/almost-300-arrested-in-joint-uae-us-chinese-crackdown-on-financial-crime/. تم التحقق في 21 نوفمبر 2026.

S46 The National، "UAE leads 39 billion USD global digital fraud crackdown with more than 900 arrests"، 22 أكتوبر 2026. https://thenationalnews.com/news/uae/2026/10/22/uae-leads-39-billion-global-digital-fraud-crackdown-with-more-than-900-arrests. تم التحقق في 21 نوفمبر 2026.

S47 11، "Dubai Police warn of rise in fake calls posing as officials and banks"، Gulf News، أبريل 2026. https://gulfnews.com/uae/crime/dubai-police-warn-of-rise-in-fake-calls-posing-as-officials-and-banks-1.500503458. تم التحقق في 21 نوفمبر 2026.

S48 Khaleej Times، تحذير شرطة دبي من روابط مزيفة لحماية المستهلك، 7 يوليو 2026. https://www.khaleejtimes.com/uae/dubai-police-fake-consumer-protection-links-banking-scam-warning. تم التحقق في 21 نوفمبر 2026.

S49 الإمارات اليوم، تحذير شرطة دبي من متصلين ينتحلون صفة موظفين في إدارة الأزمات (بالعربية)، 2 مارس 2026. https://www.emaratalyoum.com/local-section/accidents/2026-03-02-1.2020925. تم التحقق في 21 نوفمبر 2026.

S50 Khaleej Times، تحذير شرطة أبوظبي من حسابات وهمية على وسائل التواصل الاجتماعي، 25 أبريل 2026. https://www.khaleejtimes.com/uae/fake-social-media-accounts-visa-concert-ticket-property-scam. تم التحقق في 21 نوفمبر 2026.

S51 Sharjah24، قبض شرطة الشارقة على متهمين في عملية احتيال بانتحال الهوية عبر الوصول عن بُعد، 5 يوليو 2026. https://sharjah24.ae/en/Articles/2026/07/05/mm07. تم التحقق في 21 نوفمبر 2026.

S52 23، "Dubai Police arrest gang over shopping website scam"، Khaleej Times، أكتوبر 2026. https://www.khaleejtimes.com/crime/dubai-police-arrest-gang-shopping-website-scam-steal-bank-details. تم التحقق في 21 نوفمبر 2026.

S53 Khaleej Times، تحذير سلطة دبي للخدمات المالية (DFSA) من عمليات احتيال إلكترونية جديدة وشركات وهمية، 9 مارس 2026 (تنبيه DFSA بتاريخ 5 مارس). https://www.khaleejtimes.com/uae/dubai-regulator-warns-fresh-online-scams-fake-firms-dfsa-permit. تم التحقق في 21 نوفمبر 2026.

S54 Sharjah24، اعتماد مجلس الوزراء الإماراتي إنشاء مجلس الأمن السيبراني لحكومة دولة الإمارات، 29 نوفمبر 2020. https://sharjah24.ae/en/Articles/2020/11/29/VP-approves-UAE-Environment-Policy-UAE-Cybersecurity-Council-and-UAE-National-Media-Team. تم التحقق في 21 نوفمبر 2026.

S55 "World Economic Forum recognises UAE PASS as global digital government model"، Zawya (WAM)، (صفحة غير مؤرّخة). https://www.zawya.com/en/business/world-economic-forum-recognises-uae-pass-as-global-digital-government-model-402881. تم التحقق في 21 نوفمبر 2026.

S56 Federal Decree-Law No. (34) of 2021 on Countering Rumors and Cybercrimes، نص إنجليزي يستضيفه سوق أبوظبي العالمي (صدر في 20 سبتمبر 2021؛ نافذ منذ 2 يناير 2022). https://assets.adgm.com/download/assets/Federal%2BDecreeLaw%2BNo%2B34%2Bof%2B2021%2BOn%2BCountering%2BRumors%2Band%2BCybercrimes.pdf/7b3c845c864f11ef8ccdca0b2c1f6c13. تم التحقق في 21 نوفمبر 2026.

S57 Gulf News, "UAE overhauls bank risk rules: 4-hour reporting, cyber tests and tougher penalties"، آخر تحديث 15 سبتمبر 2026. https://gulfnews.com/business/banking/uae-overhauls-bank-risk-rules-4-hour-reporting-cyber-tests-and-tougher-penalties-1.500675080. تم التحقق في 21 نوفمبر 2026.

S58 Check Point Research, "Interplay between Iranian targeting of IP cameras and physical warfare in the Middle East"، 4 مارس 2026. https://research.checkpoint.com/2026/interplay-between-iranian-targeting-of-ip-cameras-and-physical-warfare-in-the-middle-east/. تم التحقق في 21 نوفمبر 2026.

S59 NIST NVD, CVE-2017-7921 (كاميرات Hikvision، مصادقة غير سليمة؛ CVSS 3.1 9.8؛ أُضيفت إلى CISA KEV في 5 مارس 2026). https://nvd.nist.gov/vuln/detail/CVE-2017-7921. تم التحقق في 21 نوفمبر 2026.

S60 NIST NVD, CVE-2021-33044 (أجهزة Dahua، تجاوز المصادقة؛ CVSS 3.1 9.8؛ أُضيفت إلى CISA KEV في 21 أغسطس 2024). https://nvd.nist.gov/vuln/detail/CVE-2021-33044. تم التحقق في 21 نوفمبر 2026.

S61 Netcraft, "Middle East crisis: opportunistic fraud"، 10 مارس 2026. https://netcraft.com/blog/middle-east-crisis-opportunistic-fraud. تم التحقق في 21 نوفمبر 2026.

S62 Khaleej Times, تقرير عن شبكة رسائل نصية وهمية للمخالفات المرورية عبر الإمارات، 11 أبريل 2026. https://www.khaleejtimes.com/uae/crime/dh4-traffic-fine-cross-emirate-fraud-network-busted-over-fake-sms-scam. تم التحقق في 21 نوفمبر 2026.

S63 Gulf News, "UAE warns against phone scams, fake websites impersonating ICP logo"، 30 أبريل 2026. https://gulfnews.com/uae/government/uae-warns-against-phone-scams-fake-websites-impersonating-icp-logo-1.500524560. تم التحقق في 21 نوفمبر 2026.

S64 Palo Alto Networks Unit 42, موجز تهديدات عن النشاط السيبراني الإيراني في 2026، 17 أبريل 2026. https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/. تم التحقق في 21 نوفمبر 2026.

S65 The National, تقرير عن انكشاف وثائق حضور مؤتمر مالي، 18 فبراير 2026. https://www.thenationalnews.com/ (رابط المقال محجوب). تم التحقق في 21 نوفمبر 2026.

S66 DeXpose, تقرير عن ادعاء ضد جهة جمركية إماراتية، 22 أغسطس 2026. https://www.dexpose.io/ (رابط المقال محجوب). تم التحقق في 21 نوفمبر 2026.

S67 Gulf News، "A hacker accessed sensitive UAE-linked systems then demanded $5m"، 15 سبتمبر 2026. https://gulfnews.com/living-in-uae/safety-security/a-hacker-accessed-sensitive-uae-linked-systems-then-demanded-5m-1.500675569. تم التحقق في 21 نوفمبر 2026.

S68 CISA (ICS-CERT)، النشرة ICSA-17-124-01، كاميرات IP من 4 Hikvision (CVE-2017-7921)، مايو 2017. https://www.cisa.gov/news-events/ics-advisories/icsa-17-124-01. تم التحقق في 21 نوفمبر 2026.

S69 Dahua، النشرة الأمنية DHCC-SA-202106-001، تجاوز مصادقة الهوية في بعض منتجات Dahua (CVE-2021-33044)، 1 سبتمبر 2021، حُدّثت في 15 نوفمبر 2021. https://www.dahuasecurity.com/about-dahua/trust-center/dahua-psirt/dhcc-sa-202106-001:security-advisory---identity-authentication-bypass-vulnerability-found-in-some-dahua-products. تم التحقق في 21 نوفمبر 2026.

الملحق D. مسرد المصطلحات

- **Blackhole**: مصدر بيانات Brandefense الخاص بالجرائم السيبرانية، ويغطي المنشورات والأجهزة المصابة وبيانات الاعتماد وبيانات البطاقات.
- **Ransompedia**: قاعدة بيانات Brandefense لبرامج الفدية؛ وتسجّل الإدراجات فيها ادعاءات إجرامية.
- **Atlas**: نظام Brandefense لتقييم الانكشاف الخارجي؛ وتتراوح الدرجات من 0 (لم يُرصد شيء) إلى 100.
- **الجهاز المصاب (Infected device)**: جهاز مصاب ببرمجيات خبيثة لسرقة المعلومات تربطه Brandefense بنطاق المؤسسة. ووصف "موظف" تصنيف من Brandefense، لا علاقة عمل مُتحقَّق منها.
- **إدراج في سوق بيانات الاعتماد (Credential-market listing)**: بيانات اعتماد مرتبطة بالنطاق معروضة في سوق خاضعة للمراقبة وقت الفحص.
- **قائمة Combolist**: قائمة بأزواج أسماء الدخول وكلمات المرور جُمعت من مصادر متنوعة؛ ويتفاوت عمرها وصلاحيتها.
- **سجل برمجيات سرقة المعلومات (Stealer log)**: بيانات تلتقطها برمجيات خبيثة لسرقة المعلومات من جهاز ما.
- **روبوت الفحص (Checker bot)**: روبوت يختبر البطاقات المسروقة عبر بوابات الدفع ويعرض النتيجة.
- **برمجيات المسح التدميرية (Wiper)**: برمجيات خبيثة تدمّر البيانات بدلاً من تشفيرها طلباً للفدية.
- **حساب وسيط لتمرير الأموال (Mule account)**: حساب مصرفي أو محفظة يُعار أو يُباع لتحريك عائدات الاحتيال.
- **التحقق من هوية العميل (KYC)**: فحوص الهوية عند فتح الحساب. وتبيع "خدمات KYC" حسابات اجتازت هذه الفحوص بالفعل.
- **رابط فحص التوفّر (Availability-check link)**: رابط إلى خدمة عامة تختبر ما إذا كان موقع ما يستجيب من عدد قليل من المواقع الجغرافية. وهو يلتقط لحظة بعينها، لا انقطاعاً للخدمة.
- **الاختراق والتسريب (Hack-and-leak)**: عملية تنشر مواد مسروقة لإلحاق الضرر أو ممارسة الضغط، وتصحبها أحياناً ادعاءات تدميرية.
- **بطاقة المنشور (Post card)**: نسخة منقّحة من منشور واحد على الويب المظلم، تتضمن المنصة والتاريخ والاسم المستعار واللغة، وما يثبته المنشور وما لا يثبته.
- **إعادة النشر (Relay)**: قناة أو روبوت تابع لطرف ثالث يعيد نشر ادعاء جهة فاعلة أخرى. وإعادة النشر دليل أضعف من منشور الجهة الفاعلة نفسها.
- **DMARC / SPF / DKIM**: معايير لمصادقة البريد الإلكتروني. ويحدد DMARC للجهات المستقبِلة كيفية التعامل مع البريد الذي يفشل في المصادقة.
- **DNSSEC**: تواقيع تتيح لخوادم الحلّ التحقق من إجابات DNS.
- **TLP:CLEAR**: يجوز تداوله دون قيود، مع بقاء الالتزامات القانونية الأخرى سارية.
- **النطاق الشبيه (Lookalike domain)**: نطاق رُصد حديثاً يشبه نطاق المؤسسة؛ مرشّح للتصيّد الاحتيالي، لا موقع تصيّد مؤكد.

- **بيانات البطاقات المنسوخة (Card dumps)**: بيانات شرائط ممغنطة منسوخة تُستخدم لاستنساخ البطاقات وتسييلها بحضور البطاقة.
- **الإدراج المقبول (Accepted listing)**: إدراج في موقع تسريب يحتفظ به Ransompedia بعد استبعاد الإدراجات المرفوضة والمكررة.
- **التقنيات التشغيلية (OT)**: أنظمة تدير عمليات مادية، مثل الكهرباء والمياه والتحكم الصناعي.
- **HSTS**: ترويسة ويب تطلب من المتصفحات استخدام HTTPS فقط.
- **منتهي الدعم (End-of-life)**: برمجيات لم تعد تتلقى تحديثات أمنية من مورّدها.

عن هذا التقرير

أعدّه Odin by Brandefense. اكتمل الإصدار 1.0 في 21 نوفمبر 2026. تاريخ إقفال البحث: 20 نوفمبر 2026 للمنشورات وإدراجات برامج الفدية والتقارير العامة؛ وقُرئت بيانات الانكشاف في 21 نوفمبر 2026. يمنح التقرير الأولوية لبيانات Brandefense الخاصة، ويفصل الادعاءات الإجرامية عن الحوادث المُثبتة بشكل مستقل، ولا يدّعي أنه حصر كامل للجرائم السيبرانية التي تطال الإمارات. لا يتخذ المؤلفون أي موقف من سياسات أي حكومة، وتُنقل الإسنادات كما ترد في مصادرها. تصف التوصيات ما يمكن أن تفعله المؤسسات، ولا تقرّر أن أي مؤسسة قد فعلته أو لم تفعله. يتوفر التقرير بنسخة عربية؛ وعند وجود اختلاف بين النسختين، تسود النسخة الإنجليزية.

© 2026 Brandefense. جميع الحقوق محفوظة.