# Kaspersky Threat Analysis

Kaspersky Research Sandbox

Kaspersky Threat Attribution Engine

Kaspersky Similarity

واجِهوا المستقبل بأمان kaspersky

# Kaspersky Threat Analysis

في مواجهة تهديد إلكتروني محتمل، قد تكون القرارات التي تتخذها، ومدى قدرتك على اتخاذها، عاملاً حاسمًا. ومن المستحيل منع الهجمات الموجهة اليوم باستخدام أدوات مكافحة الفيروسات التقليدية فقط. ولا تستطيع محركات تطبيقات مكافحة الفيروسات سوى إيقاف التهديدات المعروفة ومشتقاتها، بينما تستخدم الجهات التي تشن التهديدات المعقدة جميع الوسائل الممكنة والمتوفرة لديها لتجنب الاكتشاف الآلي. ويزداد بشكل ملحوظ عدد تنبيهات الأمان التي تعالجها مراكز عمليات الأمان كل يوم. ومع كمية عينات البرامج الضارة التي يتم إنشاؤها يوميًا، يصبح تحديد أولويات التنبيه بشكل فعال وفرزها والتحقق من صحتها أمرًا غير ممكن تقريبًا.

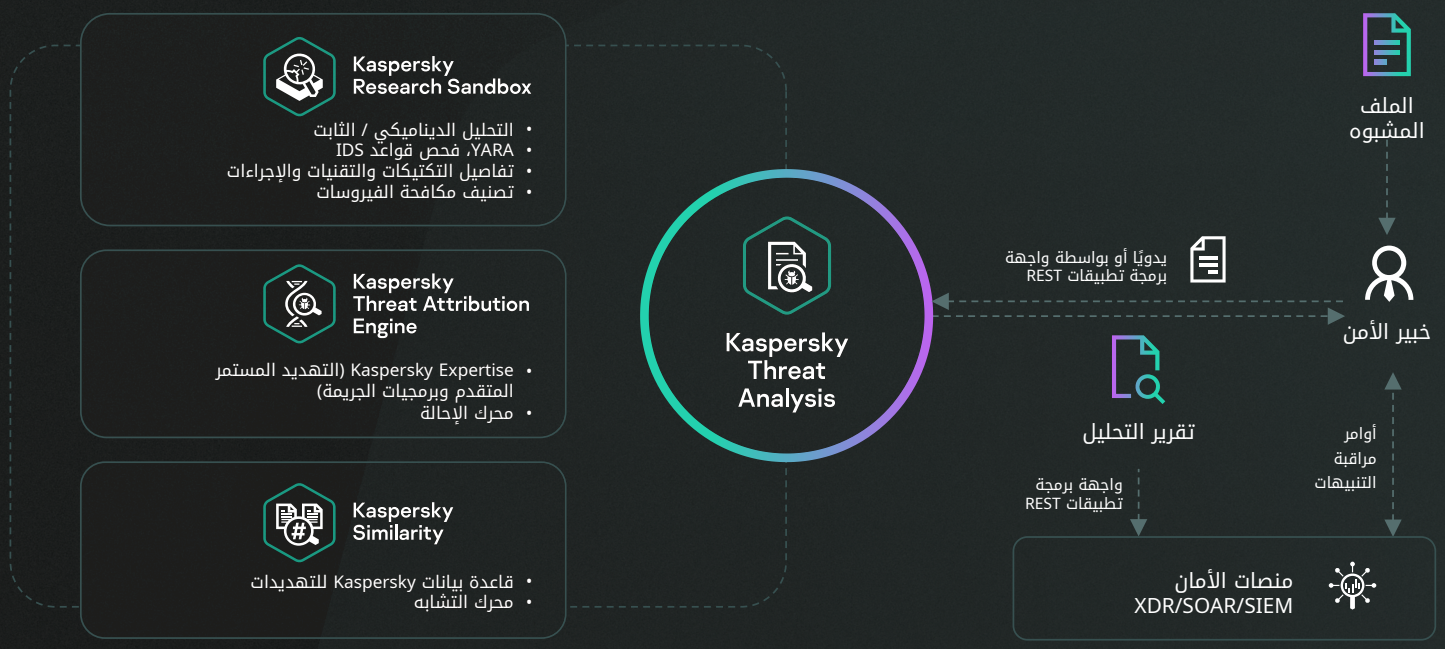
Kaspersky Threat Analysis

يوفر الجمع بين معلومات التهديد والتحليل الديناميكي وتحديد مصدر التهديد وتقنيات التشابه أداة قوية لاكتشاف الكائنات الضارة التي لم يسبق رؤيتها. ولمساعدة الباحثين في مجال الأمان على البقاء على اطلاع بالتهديدات الحالية والناشئة، توفر Kaspersky إطارًا واحدًا مرنًا لأتمتة التحليل الروتيني للملفات المشبوهة.

بالإضافة إلى تقنيات تحليل التهديدات التقليدية مثل الاختبار في وضع الحماية، يزودك حل Kaspersky Threat Analysis بأحدث تقنيات تحديد المصدر والتقنيات المشابهة ذات الصلة، وهو نهج هجين يوفر تحليلاً فعالاً للتهديدات، ما يتيح لك القدرة على اتخاذ قرارات مستنيرة بالكامل والحفاظ على أمان بنيتك التحتية.

يتم توفير حل Kaspersky Threat Analysis عبر كل من شبكة ويب موحدة وواجهات RESTful، ويتيح للمستخدمين تعيين معلمات محددة لتحليل الكائنات المشبوهة بكفاءة عالية. وتتحد أدوات تحليل التهديدات المتعددة لتتيح لك ولفريقك تحليل الموقف من جميع الزوايا، وتزويدك بتقارير كاملة وتفصيلية للاستجابة بسرعة وفعالية.

## طريقة العمل



# وضع الحماية

تم تطوير Kaspersky Research Sandbox مباشرة في مجمع بيئة الاختبار المعزولة داخل مختبرنا، وهي تقنية تشهد تطويرًا لأكثر من عقدين. وتتضمن هذه التقنية جميع المعارف المتعلقة بسلوكيات البرامج الضارة التي اكتسبناها خلال بحثنا المستمر عن التهديدات، مما يسمح لنا باكتشاف أكثر من 420000 كائن خبيث جديد كل يوم. وتقدم هذه التقنية نهجًا هجينًا، يجمع بين التحليل السلوكي وأساليب مكافحة التهرب غير القابلة للاختراق، مع تقنيات تحاكي البشر.

عند نشر هذه التقنية داخل المؤسسات، فإنها تمنع الكشف عن البيانات إلى خارجها. ويسمح Kaspersky Research Sandbox داخل المؤسسة بإنشاء بيئات تنفي مخصصة للتحليل، وتكييفها للبيئات الحقيقية، مما يؤدي إلى زيادة دقة اكتشاف التهديدات وسرعة التحقيقات.

## لماذا تستخدم هذا الحل؟

تستطيع الملفات المشبوهة، التي لم تكتشفها أدوات مكافحة الفيروسات، الكشف عن سماتها الضارة فقط أثناء سلوكها. ويسمح Kaspersky Research Sandbox بمحاكاة السلوك وتسليط الضوء على الإجراءات الخطيرة.

Kaspersky Threat Analysis

Kaspersky Research Sandbox

## تقنيات بيئات الاختبار المعزولة

أدوات تحليل ديناميكية قوية تسمح بالتحقيق في أصول عينات الملفات، وجمع بطاقات مؤشرات الاختراق بناءً على التحليل السلوكي وتحديد الكائنات الخبيثة التي لم تكتشفها أدوات مكافحة الفيروسات التقليدية.

تتوفر إصدارات سحابية ومحلية.

## مميّزات المنتج:

تُظهر درجة التهديد بناءً على المقاييس والبيانات التي يتم الحصول عليها أثناء تنفيذ الملف مستوى خطر الكائن الذي يجري تحليله

تسمح الصور المخصصة بتحليل التهديدات عبر أنظمة تشغيل Windows وتطبيقاتها (التي تنطبق فقط على البيئات الحقيقية)

التحليل الآلي للكائنات في بيئات Windows Linuxg Androidg

دعم تحليل أكثر من 200 نوع ملف مع تقديم تقارير تحليل مفصلة

تحميل العينة يدويًا وواجهة برمجة تطبيقات REST محسنة للتكامل مع سير العمل الآلي

أساليب متقدمة لمكافحة التهرب وتقنيات تحاكي البشر

دعم الوضع التفاعلي (متوقع في الربع الأول من عام 2024)

أكثر من 1000 عملية بحث فريدة لاستخراج التكتيكات والتقنيات والإجراءات بواسطة MITRE ATT&CK

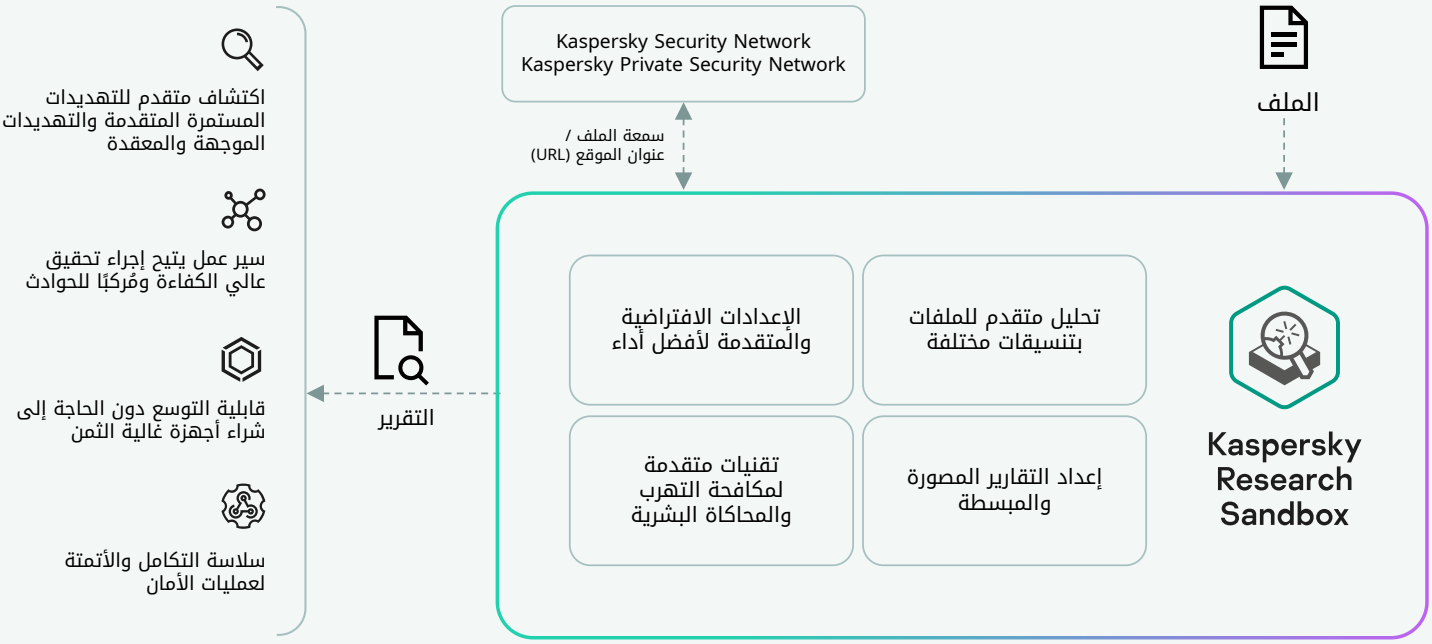
يمكن إضافة قواعد Suricata المخصصة لفحص حركة مرور الشبكة واستخدامها جنبًا إلى جنب مع قواعد Suricata

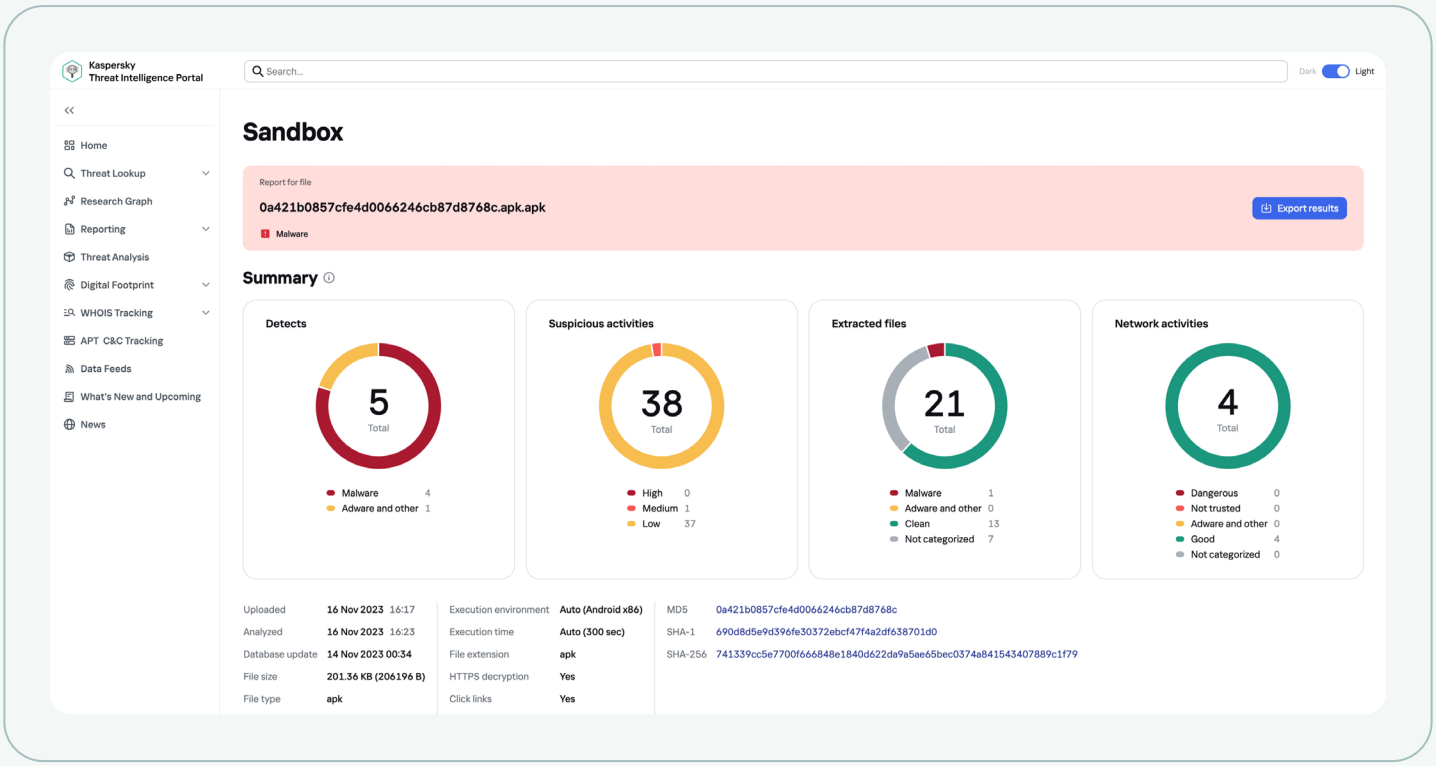
يدعم المنتج تثبيت أنظمة التشغيل لأول مرة. ويعتمد تكوين الأجهزة على الأداء المطلوب ويمكن تحديد حجمه. ويتطلب اتصال مزود خدمة إنترنت مستقلاً واحدًا على الأقل (يوصى باستخدام اتصالين أو أكثر للتغلب على الأخطاء)، بسرعة 100 ميجا بت في الثانية لكل قناة.

يعتمد حل Kaspersky Research Sandbox على تقنية مسجلة الملكية حاصلة على براءة اختراع (رقم براءة الاختراع US10339301). ومن خلال إنشاء الظروف الدقيقة التي تؤدي إلى تنفيذ البرامج الضارة، فإنه يسمح للباحثين بتحليل ملف / عنوان موقع مشبوه في محاولة واحدة.

لتجنب كشفه، قد يتحقق ملف ضار أولاً مما إذا كان موجودًا على جهاز افتراضي أو يظل غير نشط حتى يتوقف وضع الحماية عن العمل. وفي هذه الحالات، تعمل التقنية الحاصلة على براءة اختراع على تسريع تدفق الوقت داخل الجهاز الافتراضي، لذلك يتم إجبار التعليمات البرمجية الخبيثة على العمل في وقت أقرب.

## مخطط التشغيل رفيع المستوى لحل Kaspersky Research Sandbox



# تقارير تحليل مفصلة

بمجرد اكتمال التحليل، يوفر Research Sandbox تقريرًا مفصلاً عن سلوك ووظيفة العينة التي تم تحليلها، مما يسمح لك بتحديد إجراءات الاستجابة المناسبة:

| | |
|---|---|
| الملخص | معلومات عامة عن نتائج تنفيذ الملف / تصفح عنوان الموقع (URL). |
| أسماء الاكتشاف | قائمة بعمليات الاكتشاف (لمكافحة الفيروسات والسلوكية) التي تم تسجيلها أثناء تنفيذ الملف. |
| قواعد الشبكة التي تم تشغيلها | قائمة بقواعد شبكة Suricata التي تم تشغيلها أثناء تحليل حركة المرور من الكائن الذي تم تنفيذه. |
| خريطة التنفيذ | تسلسل بتمثيل بياني لأنشطة الكائن والعلاقة بينها. |
| الأنشطة المشبوهة | الأنشطة المشبوهة - قائمة بالأنشطة المشبوهة المسجلة. |
| لقطات الشاشة | مجموعة لقطات الشاشة التي تم التقاطها أثناء تنفيذ الملف / استعراض عنوان الموقع (URL). |
| صور الملفات القابل للتنفيذ المحمولة المُحملة | قائمة بصور الملفات التنفيذية القابلة للنقل المُحملة المكتشفة أثناء تنفيذ الملف / استعراض عنوان الموقع (URL). |
| عمليات الملف | قائمة عمليات الملف التي تم تسجيلها أثناء تنفيذ ملف / استعراض عنوان الموقع (URL). |
| عمليات التسجيل | قائمة بالعمليات التي تم إجراؤها على سجل نظام التشغيل التي تم اكتشافها أثناء تنفيذ الملف / استعراض عنوان الموقع. |
| عمليات المعالجة | قائمة تفاعلات الملف مع العمليات المختلفة التي تم تسجيلها أثناء تنفيذ الملف. |
| مزامنة العمليات | قائمة بعمليات كائنات المزامنة التي تم إنشاؤها (كائن المزامنة، الحدث، الإشارة) التي تم تسجيلها أثناء تنفيذ الملف / استعراض عنوان الموقع (URL). |
| الملفات التي تم تنزيلها | قائمة بالملفات التي تم استخراجها من حركة مرور الشبكة أثناء تنفيذ الملف / استعراض عنوان الموقع (URL). |
| الملفات المُسقطة | قائمة بالملفات التي تم حفظها (تم إنشاؤها أو تعديلها) بواسطة الملف الذي تم تنفيذه. |
| HTTPS/HTTP/DNS/IP/TCP/UDP وما إلى ذلك. | جلسات الشبكة / تفاصيل الطلبات التي تم تسجيلها أثناء تنفيذ الملف / استعراض عنوان الموقع (URL). |
| تفريغ حركة مرور الشبكة (PCAP) | يمكن تصدير نشاط الشبكة بتنسيق PCAP. |
| مصفوفة MITRE ATT&CK | يتم عرض جميع أنشطة العملية المحددة المسجلة أثناء المحاكاة في شكل مصفوفة MITER ATT&CK. |

# الصفات

Kaspersky Threat Attribution Engine أداة فريدة لتحليل التهديدات توفر نظرة ثاقبة حول أصل البرامج الضارة البارزة وصانعيها المحتملين. ويربط الحل بسرعة ملفًا مشبوهًا بالتهديدات المستمرة المتقدمة والأطراف والحملات المعروفة، باستخدام خوارزمية فريدة وقاعدة بيانات خاصة تضم عينات من برامج التهديدات المستمرة المتقدمة الضارة وأكبر مجموعة من الملفات النظيفة على مستوى الصناعة والتي جمعها خبراء Kaspersky على مدار 25 عامًا وأكثر.

نتتبع أكثر من 1100 جهة وحملة للتهديد ونُصدر أكثر من 200 تقرير معلومات عن التهديدات سنويًا. ويدعم بحثنا المستمر مجموعة التهديدات المستمرة المتقدمة التي تحتوي على أكثر من 80000 ملف، والتي تؤدي، جنبًا إلى جنب مع استخدام الأدوات الآلية، إلى مستويات دقيقة للغاية من تحديد المصدر.

يقدم المنتج طريقة فريدة لمقارنة العينات المماثلة مع ضمان معدلات إيجابية كاذبة قريبة من الصفر. ويمكن ربط أي هجوم جديد بسرعة ببرامج التهديدات المستمرة المتقدمة الضارة المعروفة والهجمات الموجهة السابقة ومجموعات المتسللين، مما يساعدك على التمييز بين التهديدات عالية الخطورة والحوادث الأقل خطورة، حتى تتمكن من اتخاذ تدابير وقائية في الوقت المناسب لمنع المهاجم من الحصول على موطئ قدم في نظامك . ويمكن نشر Kaspersky Threat Attribution Engine في بيئات آمنة معزولة، مما يمنع أي طرف ثالث من الوصول إلى المعلومات المعالجة والكائنات المقدمة.

## لماذا تستخدم هذا الحل؟

يسمح تحديد مصدر الملف من جهة تهديد معينة، إلى جانب معرفة جهة التهديد هذه، بمعرفة مكان هذه العينة في سلسلة تتبع الهجوم الإلكتروني الشاملة، الخاصة بهذا المهاجم. ويوفر بدوره المعرفة بمكان البحث عن مؤشرات الاختراق / مؤشرات الهجوم الأخرى وعدم تفويت الهجوم بأكمله عن طريق حظر ملف معين واحد فقط.

Kaspersky Threat Analysis

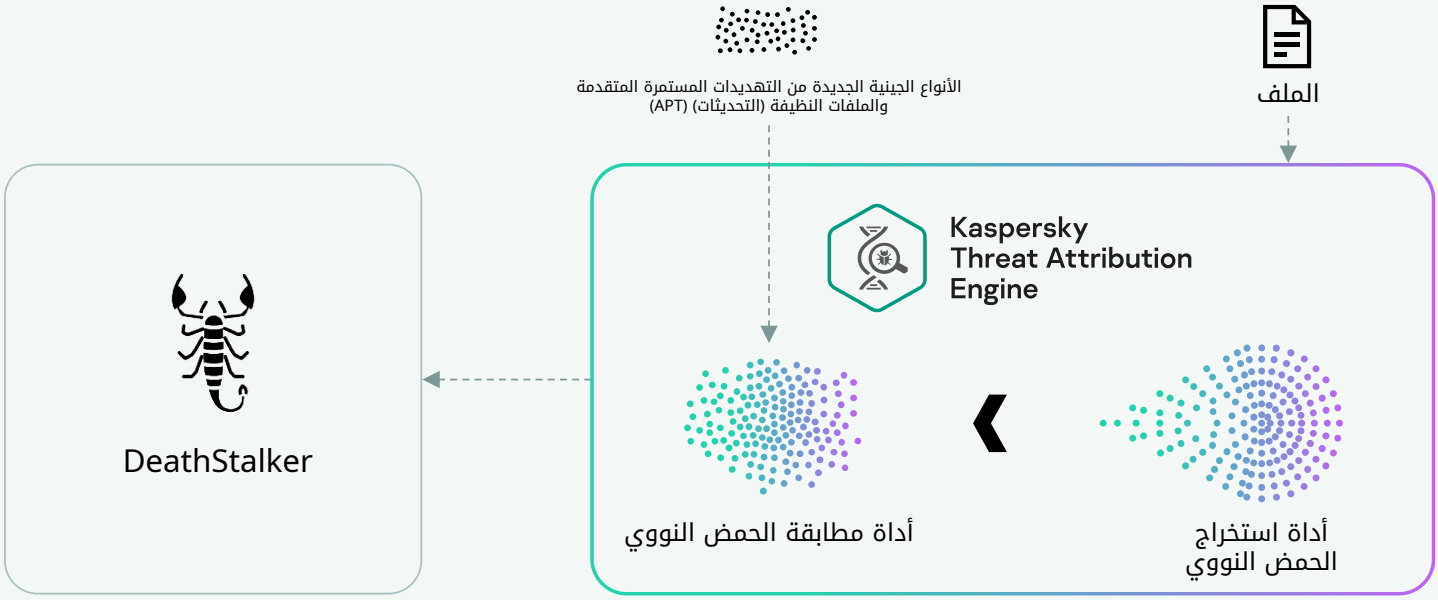
Kaspersky Threat Attribution Engine

## تحديد مصدر التهديد

يعد تعقب تهديدات أمان تكنولوجيا المعلومات وتحليلها وتفسيرها والحدّ منها باستمرار مهمة كبيرة. وبغض النظر عن كل هذه الضجة، فإن المعلومات المتعلقة بالتهديدات تتمتع بقيمة حقيقية، ويعتبر تحديد مصدر التهديد عنصرًا حاسمًا هنا.

تتوفر إصدارات سحابية ومحلية.

## مخطط التشغيل رفيع المستوى لحل Kaspersky Threat Attribution Engine



## مميّزات المنتج:

يوفر الوصول الفوري إلى مستودع البيانات المنسقة عن الآلاف من جهات التهديدات المستمرة المتقدمة والعينات والتهديدات الأوسع (عبر محرك مكافحة الفيروسات)

رؤى فريدة حول الحملات رفيعة المستوى (أكثر من 400) التي قام حقق فيها خبراء Kaspersky

السماح بترتيب أولويات التهديدات آليًا أو يدويًا وترتيب التنبيهات بشكل فعال

إضافة أطراف وعينات خاصة لإرشاد المنتج لاكتشاف العينات التي تشبه الملفات في مجموعتك الخاصة

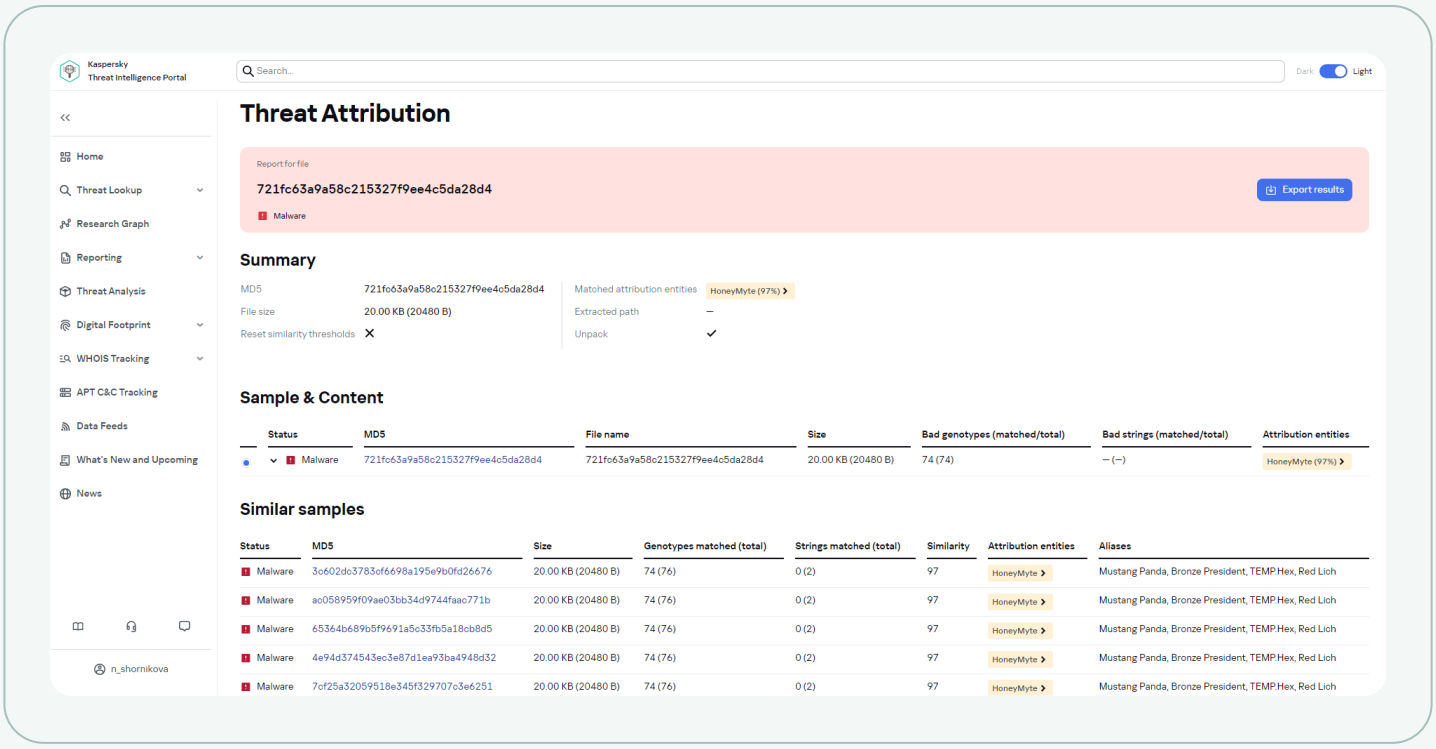
تحميل العينة يدويًا وواجهة برمجة تطبيقات REST محسنة للتكامل مع سير العمل الآلي

يدعم النشر على البنى التحتية السحابية مثل Amazon Web Services (AWS) مما يتيح الإعداد السريع للمنتج وتوفير التكاليف حيث لا توجد حاجة للاستثمار في الأجهزة مقدمًا

التصدير إلى قواعد YARA لمزيد من البحث / الفحص الآلي للملفات المشابهة أو التكامل مع حلول الجهات الخارجية

التصدير إلى تنسيق STIX 2.1 (تنسيقات TXT وJSON مدعومة أيضًا) لإجراء المزيد من التحليل الآلي لسجلات الأمان أو التكامل مع حلول الجهات الخارجية / عناصر التحكم في الأمان

وظيفة لفتح الأرشيفات المحمية بكلمة مرور باستخدام كلمات مرور مخصصة



## طريقة البحث الخاصة

لربط البرامج الضارة بكيانات مصدر التهديد، يستخدم Kaspersky Threat Attribution Engine طريقة خاصة فريدة للبحث عن الأنماط الجينية والسلاسل المتشابهة بين الملفات. تتضمن هذه الطريقة:

### تحليل العوامل الوراثية لعينة

عن طريق استخراج العناصر التالية من التعليمات البرمجية الخاصة به:

- الأنماط الجينية - أجزاء مميزة من التعليمات البرمجية الثنائية
- السلاسل - سلاسل مميزة من الأحرف

### البحث تلقائيًا في الملفات التي تم تحليلها

للأنماط الجينية والسلاسل المشابهة للأنماط الجينية وسلاسل عينات التهديد المستمر المتقدم التي سبق تحليلها، أو المرتبطة بالفعل بكيانات مصدر التهديد

### الاعتماد على الأنماط الجينية والسلاسل المماثلة

الموجودة في عينات التهديد المستمر المتقدم، مع تقديم تقرير عن أصل العينة التي تم تحليلها وكيانات مصدر التهديد ذات الصلة وأي أوجه تشابه بين هذه العينة وعينات التهديد المستمر المتقدم المعروفة

# التشابه

Kaspersky Similarity عبارة عن ميزة إضافية متاحة عبر Threat Intelligence Portal لكل من مستخدمي Kaspersky Research Sandbox وKaspersky Threat Attribution Engine، مما يساعد على تحديد الملفات التي تبدو وتتصرف بطرق مماثلة.

يجري البحث عن الملفات المماثلة وحسابها للملف الأصلي باستخدام التقنية المتطورة التي ابتكرها خبراء Kaspersky للاستفادة من أكثر من 50 نوعًا فريدًا من أنواع تجزئة التشابه. يسمح هذا بضمان نتائج تشابه دقيقة وعالية الثقة.

## لماذا تستخدم هذا الحل؟

ابحث عن البرامج الضارة المتشابهة (على سبيل المثال، المراوغة) وابحث عنها في بنيتك التحتية لتكون واثقًا من أن التغيير الطفيف في العينة، الذي أجراه المهاجم، لا يزال تحت مراقبة نظام الأمان الخاص بك. تتميز التقنية عن تحديد المصدر: حتى أنه لا يمكن العثور على ملفات ضارة متشابهة لم يتحدد مصدرها.

Kaspersky Threat Analysis

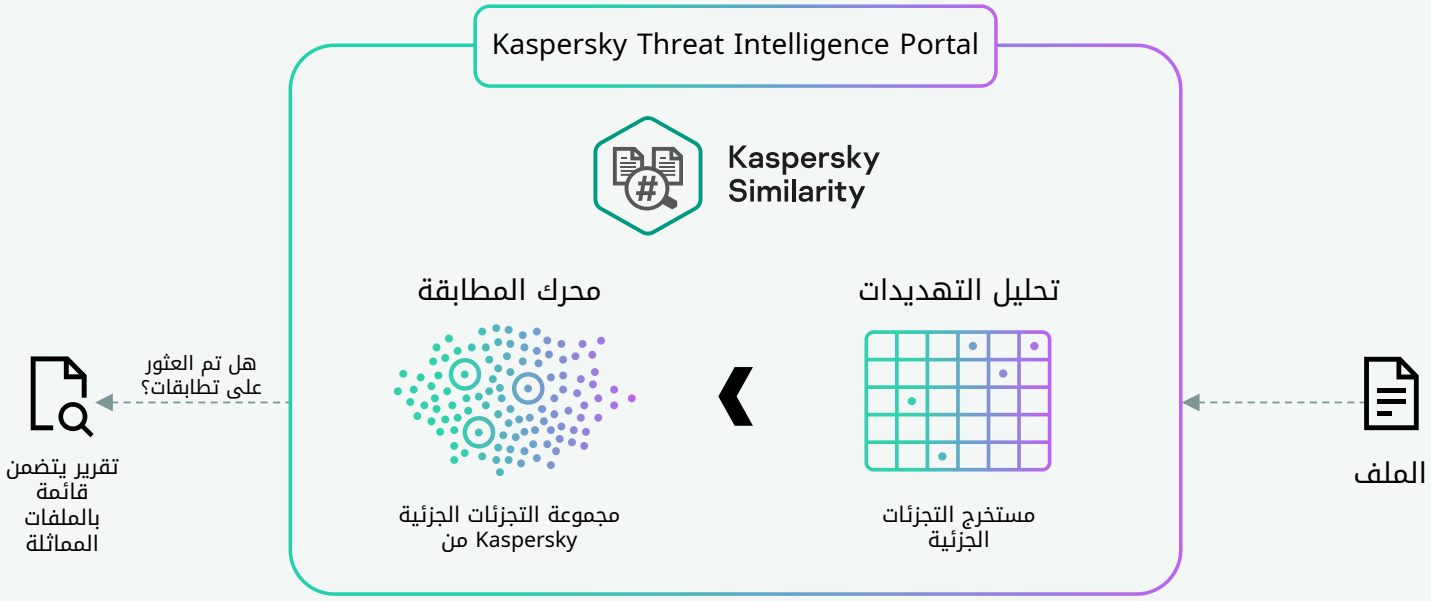
Kaspersky Similarity

## تشابه الملفات

لبناء خط دفاع فعال، ليس من الضروري دائمًا معرفة عدوك عن طريق النظر. ويسمح Kaspersky Similarity بتحديد عينات الملفات ذات الوظائف المماثلة، للحماية من التهديدات غير المعروفة والمراوغة

يتوفر الإصدار السحابي عبر Kaspersky Threat Intelligence Portal.

## مخطط العمل رفيع المستوى لحل Kaspersky Similarity



## تقارير التشابه

يحتوي كل ملف على تنسيق محدد وحزم مستخدمة وأقسام وسلاسل وجداول استيراد وما إلى ذلك. وقد أنشأ خبراء Kaspersky مجموعة من التجزئات لتحديد مدى التشابه بين الملفات المختلفة بناءً على هذه السمات. ويسمح Kaspersky Similarity للمستخدمين بإرسال ملف مشبوه، واستخراج تجزئاته الجزئية ومقارنتها مع التجزئات الجزئية من الملفات الموجودة في قاعدة بيانات التهديدات من Kaspersky. وفي حالة العثور على تطابقات، فإنه يُنشئ قائمة التجزئات لأفضل الملفات الضارة المشابهة، المعروفة بالفعل لدي Kaspersky ويتم فرزها حسب درجة التشابه. ويحتوي التقرير على السياق الإضافي مع البيانات الوصفية لكل ملف مشابه:

- ثقة التشابه
- حالة الملف (برامج ضارة أو برامج إعلانية أو غيرها)
- أسم التهديد
- الطوابع الزمنية للاكتشاف الأول والأخير
- كمية الزيارات (الاكتشافات)
- تجزئة الملف
- نوع الملف
- حجم الملف

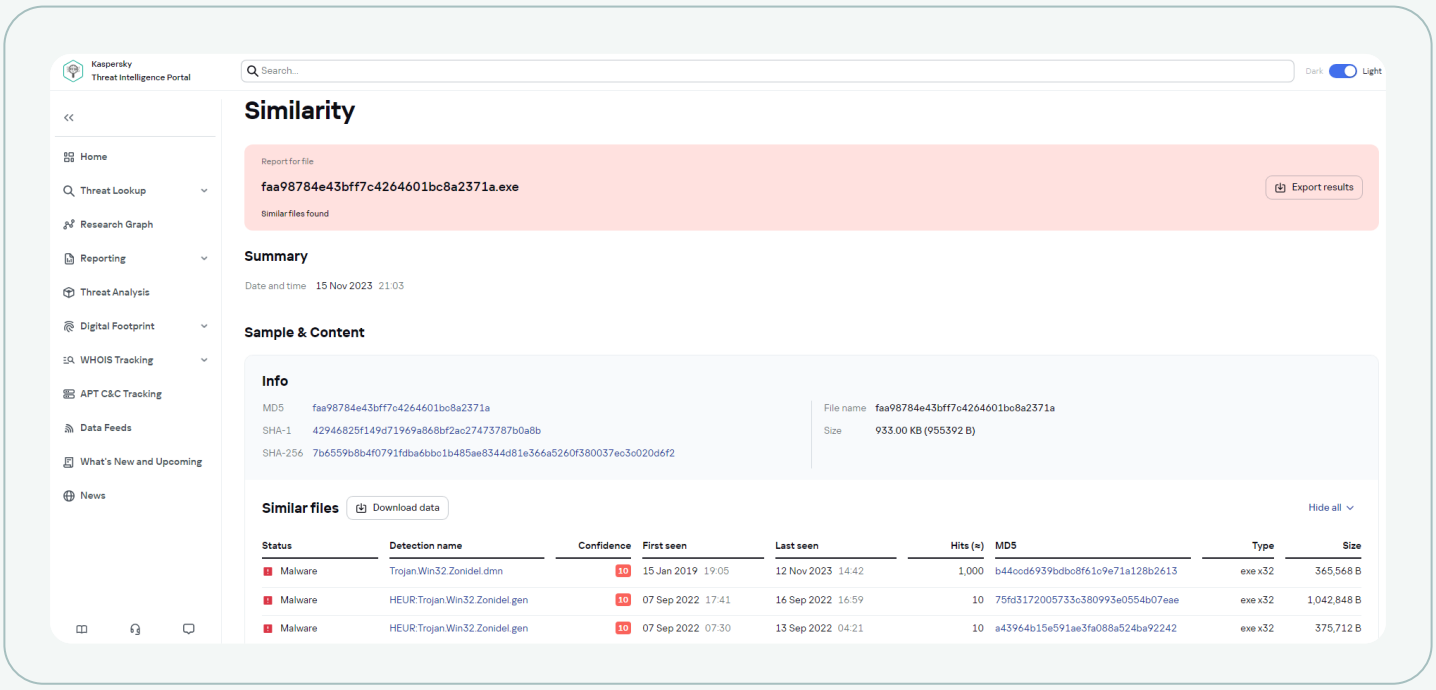
## أهم الميزات

يستفيد من واحدة من أكبر قواعد البيانات في المجال للملفات الضارة والنظيفة، والتي تم جمعها على مدار أكثر من 25 عامًا، مما يتيح أقصى قدر من التغطية للحصول على أعلى دقة مقارنة

تحميل العينة يدويًا وواجهة برمجة تطبيقات REST محسنة للتكامل مع سير العمل الآلي

يتم توفيرها لمستخدمي Kaspersky Research Sandbox Kaspersky Threat Attributiong مجانًا لتعزيز فعالية كلتا التقنيتين وتوفير معلومات شاملة عن الملف الذي يجري تحليله

يُستخدم بالفعل على نطاق واسع من قبل خبراء Kaspersky لاستكشاف التهديدات الجديدة لتوفير حماية أعلى من التهديدات في منتجاتنا، وهو ما يتم تأكيده بانتظام من خلال أعلى المعدلات المتنظمة وفقًا للاختبارات المستقلة:



## حالات استخدام Kaspersky Threat Analysis

يوفر تحليل التهديدات من Kaspersky أدوات ناضجة مختارة لاكتشاف التهديدات غير المعروفة التي يمكن تطبيقها على نطاق واسع في السيناريوهات التالية:

### الاستجابة للحوادث

اكشف التهديدات المراوغة

التحليل الثابت / الديناميكي للملفات المشبوهة

كشف علاقة برنامج ضار جديد بجهة تهديد معينة لمعرفة الخطوات الإضافية المحتملة للهجوم

### البحث عن المخاطر

استلام فحص البنية التحتية للبحث عن مؤشرات الاختراق من خلال التقرير

البحث عن التعديلات الضارة المحتملة للملفات النظيفة الشائعة

تحديد مؤشرات الاختراق المشتركة بين الملفات الضارة غير المعروفة والمعروفة

### تحليل البرامج الضارة

تحليل التهديد غير المعروف

البحث عن البرامج الضارة ذات الصلة للمساعدة في إجراء الهندسة العكسية للملفات المبهمة

Kaspersky Threat Analysis أداة بحثية مرنة تحتوي على مكونات مترابطة تتيح إجراء تقييم شامل ومتعدد الطبقات للكائنات المشبوهة لتحديد الهجمات المتقدمة وتصنيفها. ويساعد فرق مركز عمليات الأمان والباحثين الأمنيين ومحللي البرامج الضارة على البقاء على اطلاع بالتهديدات الحالية والناشئة المتعلقة بالبرامج الضارة، مما يسمح لهم بتحديد أولويات التهديدات الحرجة ومعالجتها بسرعة ومعالجتها بشكل أكثر فعالية.

# Kaspersky Threat Analysis

معرفة المزيد

#kaspersky
#bringonthefuture

me.kaspersky.com

© 2023 AO Kaspersky Lab.
العلامات التجارية المسجلة وعلامات الخدمة
مملوكة لأصحابها.