Kaspersky Research Sandbox

واجهوا المستقبل بأمان kaspersky

Kaspersky Research Sandbox

تقنيات بيئات الاختبار المعزولة

تُعد تقنيات بيئات الاختبار المعزولة أدوات قوية تسمح بالتحقيق في أصول عينة الملف، ويجمع مؤشرات الاختراق بناءً على التحليل السلوكي له واكتشاف الكائنات الضارة التي لم يسبق رؤيتها.

يُعد اتخاذ قرار مدروس بناءً على سلوك ملفٍ أو عنوان موقع على الإنترنت مع العمل في الوقت نفسه على تحليل ذاكرة العمليات وأنشطة الشبكات وما إلى ذلك، النهج الأمثل لفهم التهديدات الحالية المعقدة وأهدافها وطريقة تخصيصها للهجوم على كل مؤسسة.

تستخدم البرامج الضارة في عصرنا الحاضر مجموعة متنوعة كاملة من الطرق لتجتنب تنفيذ تعليماتها البرمجية إذا كان فعل ذلك سيؤدي إلى كشف نشاطها الخبيث، إذا كان النظام لا يفي بالمعلمات المطلوبة، فإن البرنامج الضار سيدمر نفسه بلا شك مع عدم ترك أي أثر له. كي يتم تنفيذ الكود الضار، فإن بيئة العزل والفحص يجب أن تكون قادرة على محاكاة السلوك الطبيعي للمستخدم النهائي بدقة

تم تطوير Kaspersky Research Sandbox مباشرة في مجمع بيئة الاختبار المعزولة داخل مختبرنا، وهي تقنية تشهد تطويرًا لأكثر من عقدٍ من الزمان، وتتضمن هذه التقنية جميع المعارف المتعلقة بسلوكيات البرامج الضارة التي اكتسبناها خلال بحثنا المستمر عن التهديدات، مما يسمح لنا باكتشاف أكثر من 380000 كائن خبيث جديد كل يوم. وعند نشر هذه التقنية القوية داخل المؤسسات، فإنها تمنع الكشف عن البيانات إلى خارجها.

تقدم هذه التقنية نهجًا هجينًا، يجمع بين التحليل السلوكي وأساليب مكافحة التهرب غير القابلة للاختراق، مع تقنيات تحاكي البشر. ويسمح Kaspersky Research Sandbox أيضًا بتخصيص صور النظام لتحليلها، وتكييفها وفقًا للبيئات الحقيقية، مما يؤدي إلى زيادة دقة اكتشاف التهديدات وسرعة التحقيقات.

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
- الإرسال اليدوي للملف / عنوان الموقع وواجهة برمجة تطبيقات RESTful
- أساليب متقدمة لمكافحة التهرب وتقنيات تحاكي البشر
- يضمن النشر داخل المؤسسات عدم كشف أي بيانات خارج المؤسسة
- يدعم المنتج تثبيت أنظمة التشغيل لأول مرة ويمكن تحديد حجمه بسهولة اعتمادًا على الأداء المطلوب
- يمكن إضافة قواعد Suricata المخصصة لفحص حركة مرور الشبكة واستخدامها جنبًا إلى جنب مع قواعد Suricata المقدمة الجاهزة
- دعم تحليل أكثر من 100 نوع ملف مع تقديم تقارير تحليل مفصلة

بنية Kaspersky Research Sandbox عالية المستوى

يدعم المنتج تثبيت أنظمة التشغيل لأول مرة. ويعتمد تكوين الأجهزة على الأداء المطلوب ويمكن تحديد حجمه. ويتطلب اتصال شبكة بسعة 100 ميجابت في الثانية لكل قناة واتصال مزود خدمة إنترنت مستقل واحد على الأقل (يوصى باستخدام اثنين من مزودي خدمة الإنترنت أو أكثر للتغلب على الأعطال). ويجب أن يكون مزود خدمة الإنترنت على علم وجاهز لحركة المرور الضارة.

يعتمد منتج 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.

قد لا تُظهر البرامج الضارة سلوكها الضار إذا كانت تستهدف تطبيقًا معينًا غير موجود في وضع الحماية. وللتغلب على هذا التحدي، يجب على الباحثين مراجعة السجلات وفهم ما هو مفقود وإضافته إلى جهاز افتراضي وتشغيل هذه العملية مرة أخرى. وعندما تحاول البرامج الضارة الوصول إلى أحد التطبيقات، يعترض النظام الحاصل على براءة اختراع هذه المحاولة. ولا ينتظر حتى انتهاء تنفيذ الملف، لكنه يُوقف مؤقتًا عملية إنشاء التطبيق المطلوب بالإضافة إلى المحتوى.

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.

أسماء الاكتشاف

قائمة بعمليات الاكتشاف (المضادة للفيروسات 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.

صور الملفات التنفيذية القابلة للنقل المُحملة

قائمة بصور الملفات التنفيذية القابلة للنقل المُحملة المكتشفة أثناء تنفيذ **الملف / استعراض عنوان الموقع**.

عمليات الملف

قائمة عمليات الملف التي تم تسجيلها أثناء تنفيذ ملف / استعراض عنوان الموقع.

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 موقع الويب.

الملفات التي تم تنزيلها

قائمة بالملفات التي تم استخراجها من حركة مرور الشبكة أثناء تنفيذ الملف / استعراض عنوان الموقع.

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

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.

Kaspersky Research Sandbox هو الأداة المفضلة للاكتشاف التهديدات غير المعروفة. وهو منتج أكثر نضجًا وأكثر تركيزًا على التهديدات المتقدمة من أي حل آخر.

me.kaspersky.com