Kaspersky Research Sandbox

Kaspersky Threat Attribution Engine

Kaspersky Similarity

Kaspersky Tehdit Analizi

kaspersky geleceği yakalayın

Kaspersky Tehdit Analizi

Kaspersky Threat Analysis

Potansiyel bir siber tehditle karşı karşıya kaldığınızda, verdiğiniz kararlar ve bu kararları ne kadar iyi verebildiğiniz kritik öneme sahip olabilir. Günümüzün hedefli saldırılarını yalnızca geleneksel anti virüs araçlarıyla önlemek mümkün değildir. Anti virüs motorları sadece bilinen tehditleri ve bunların türevlerini durdurma kabiliyetine sahipken gelişmiş tehdit aktörleri otomatik tespiti atlatmak için ellerindeki tüm araçları kullanır. Her gün SOC'leri tarafından işlenen güvenlik uyarılarının sayısı katlanarak artıyor. Her gün üretilen kötü amaçlı yazılım örneklerinin miktarı göz önüne alındığında, etkili uyarı önceliklendirme, öncelik belirleme ve doğrulama neredeyse imkansız hale gelmektedir.

Tehdit istihbaratı, dinamik analiz, tehdit ilişkilendirme ve benzerlik teknolojilerinin birleştirilmesi, daha önce görülmemiş kötü niyetli nesnelerin tespiti için güçlü bir araç sağlar. Kaspersky, güvenlik araştırmacılarının var olan ve yeni ortaya çıkan tehditler hakkında bilgi sahibi olmalarına yardımcı olmak için şüpheli dosyaların rutin analizini otomatikleştiren tek bir esnek çerçeve sunuyor.

Kaspersky Tehdit Analizi, sandboxing gibi geleneksel tehdit analizi teknolojilerine ek olarak sizi en gelişmiş ilişkilendirme ve ilgili benzerlik teknolojileriyle donatır. Etkili tehdit analizi sağlayan bu hibrit yaklaşım, tamamen bilinçli kararlar verebilir ve böylece altyapınızı güvende tutabilirsiniz.

Kaspersky Tehdit Analizi, hem birleşik web hem de RESTful arayüzleri aracılığıyla sunulur ve kullanıcıların şüpheli nesneleri yüksek verimlilikle analiz etmek için belirli parametreler ayarlamasına olanak tanır. Çoklu tehdit analizi araçları bir araya gelerek, sizin ve ekibinizin durumu hızlı ve etkili bir şekilde yanıt vermek için eksiksiz ve ayrıntılı raporlarla tüm açılardan analiz etmenizi sağlar.

Nasıl çalışır?

Sandboxing teknolojileri

dosya örneği kökenlerini araştırmaya, davranışsal analize dayalı IOC'leri toplamaya ve geleneksel anti virüs araçları tarafından tespit edilmeyen kötü amaçlı nesneleri belirlemeye olanak tanıyan güçlü dinamik analiz araçlarıdır.

Bulut ve şirket içi sürümleri mevcuttur.

Koruma

Kaspersky Research Sandbox, doğrudan yirmi yıldan fazla bir süredir gelişen bir teknoloji olan laboratuvar kullanımına yönelik korumalı alan kompleksimizden geliştirilmiştir. Kesintisiz tehdit araştırmalarımız boyunca edindiğimiz kötü amaçlı yazılım davranışları hakkındaki tüm bilgileri bir araya getirirken aynı zamanda her gün 420.000'den fazla yeni kötü amaçlı nesneyi tespit etmemizi sağlar. Davranış analizini ve son derece sağlam atlatma önleme tekniklerini insan simülasyonu teknolojileriyle birleştiren hibrit bir yaklaşım sunar.

Tesislerde kullanıldığında bu teknoloji, verilerin kuruluş dışında açığa çıkarılmasını da önler. Kaspersky Research Sandbox, analiz için gerçek ortamlara uyarlanmış özel yürütme ortamları oluşturmaya da olanak tanıyarak tehdit tespitinin doğruluğunu ve araştırma hızını artırır.

Neden kullanılmalı?

Anti virüs araçları tarafından tespit edilmeyen şüpheli dosyalar, kötü niyetli özelliklerini yalnızca davranışları sırasında ortaya çıkarabilir. Kaspersky Research Sandbox, davranışı taklit ederek tehlikeli eylemlerin ortaya çıkmasını sağlar.

Ürünün öne çıkan özellikleri

Windows, Linux ve Android ortamlarında otomatik hâle getirilmiş nesne analizi

Özel görüntüler, Windows işletim sistemlerinde ve uygulamalarında (yalnızca gerçek ortamlar için geçerli olanlarda) tehdit analizi sağlar

Dosya yürütme sırasında elde edilen ölçümler ve verilere dayalı tehdit puanı, analiz edilen nesnenin tehlike düzeyini gösterir

Gelişmiş atlatma karşıtı teknikler ve insan simülasyonlu teknolojiler

Manuel örnek yükleme ve otomatik iş akışlarıyla entegrasyon için geliştirilmiş REST API

Ayrıntılı analiz raporlarıyla 200'den fazla dosya türünün analizi için destek

Ağ trafiğini taramak için özel Suricata kuralları eklenebilir ve Suricata kurallarıyla birlikte kullanılabilir

MITRE ATT&CK tarafından TTP'lerin çıkarılması için 1000'den fazla benzersiz av

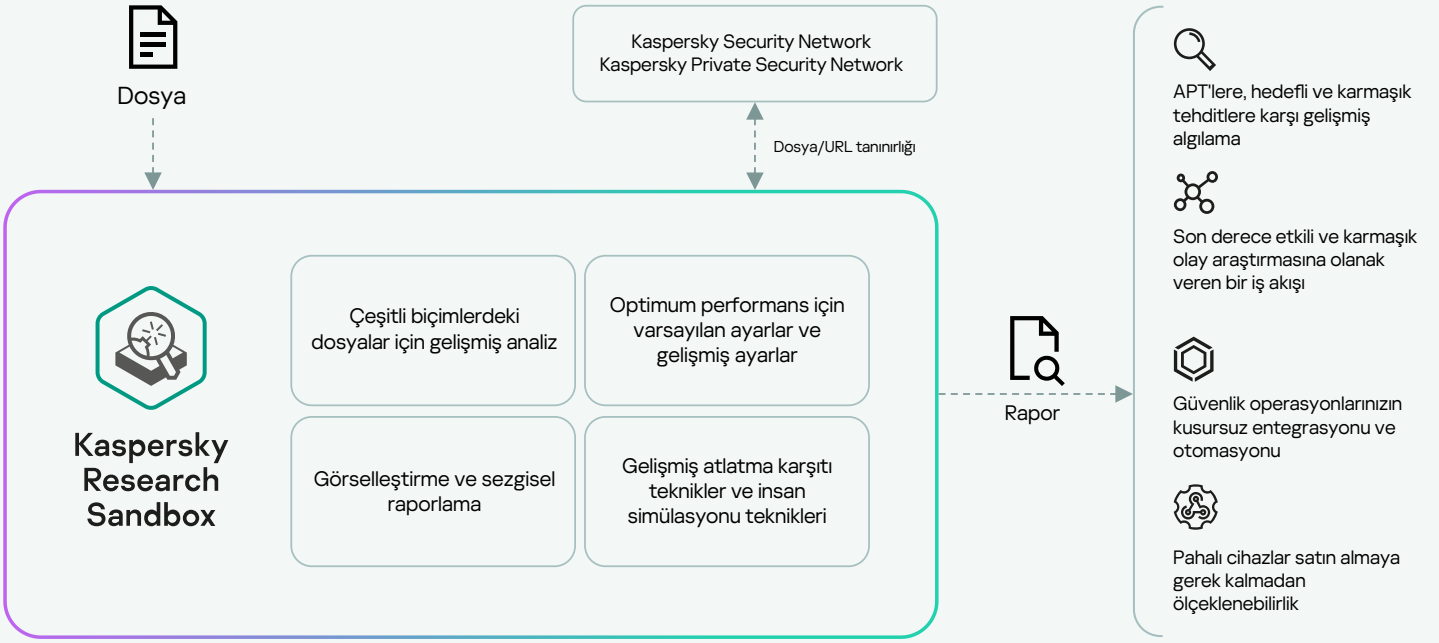
Etkileşimli mod desteği (2024'ün ilk çeyreğinde bekleniyor)

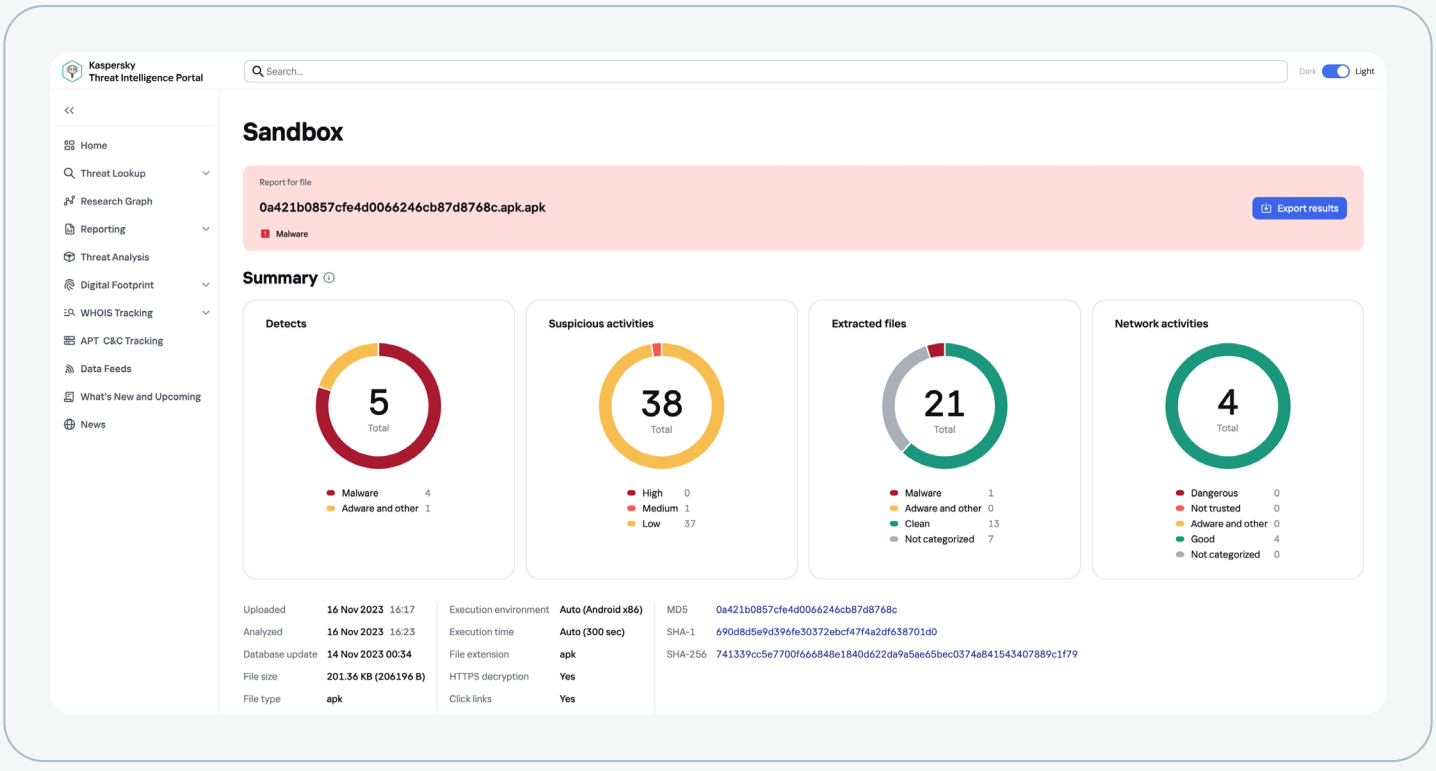
Ürün, işletim sistemi/yazılım içermeyen dağıtımı destekler. Donanım yapılandırması, gerekli performansa bağlıdır ve ölçeklenebilir. En az bir bağımsız ISP bağlantısı (hata toleransı için iki veya daha fazlası önerilir), her kanal için 100 Mbps gerektirir.

Kaspersky Research Sandbox, patentli tescilli bir teknolojiye dayanmaktadır (patent no. US10339301). Kötü amaçlı yazılımın yürütülmesini tetikleyen koşulları bire bir oluşturarak araştırmacıların şüpheli bir dosyayı/URL'yi tek bir denemede analiz etmelerine olanak tanır.

Saldırılara maruz kalmayı önlemek için kötü amaçlı bir dosya, ilk olarak sanal bir makinede olup olmadığını araştırabilir veya korumalı alan çalışmamaya başlayana kadar pasif durumda kalabilir. Bu gibi durumlarda patentli teknoloji, sanal makine içindeki zaman akışını hızlandırır ve böylece kötü amaçlı kodun daha erken yürütülmesini sağlar.

Kaspersky Research Sandbox yüksek seviyeli çalışma mimarisi





Ayrıntılı analiz raporları

Research Sandbox, analiz tamamlandıktan sonra analiz edilen örneğin davranışı ve işlevselliği hakkında ayrıntılı bir rapor sağlayarak uygun müdahale prosedürlerini tanımlamanıza olanak tanır:

Özet	Bir dosyanın yürütülmesi/URL'de göz atma sonuçları hakkında genel bilgiler.
Tespit isimleri	Dosya yürütme sırasında kaydedilen tespitlerin (hem AV hem davranışsal) bir listesi.
Tetiklenen ağ kuralları	Yürütülen nesneden gelen trafiğin analizi sırasında tetiklenen ağ Suricata kurallarının bir listesi.
Yürütme haritası	Grafiksel olarak temsil edilen nesne faaliyetlerinin dizisi ve bunlar arasındaki ilişki.
Şüpheli etkinlikler	Şüpheli etkinlikler - kaydedilen şüpheli etkinliklerin bir listesi.
Ekran görüntüleri	Dosya yürütme/URL'de göz atma sırasında alınan ekran görüntüleri.
Yüklenen PE görüntüleri	Dosya yürütme/URL'de göz atma sırasında algılanan yüklü PE görüntülerinin bir listesi.
Dosya işlemleri	Dosya yürütme/URL'de göz atma sırasında kaydedilen dosya işlemlerinin bir listesi.
Kayıt işlemleri	Dosya yürütme/URL'de göz atma sırasında algılanan, işletim sistemi kayıt defterindeki gerçekleştirilen işlemlerin bir listesi.
Süreç işlemleri	Dosyanın, dosya yürütülmesi sırasında kaydedilen çeşitli süreçlerle olan etkileşimlerinin bir listesi.
Senkronizasyon işlemleri	Dosya yürütme/URL'de göz atma sırasında kaydedilmiş, oluşturulan senkronizasyon nesnelerinin (mutex, olay, semafor) işlemlerinin bir listesi.
İndirilen dosyalar	Dosya yürütme/URL'de göz atma sırasında ağ trafiğinden çıkarılan dosyaların bir listesi.
Bırakılan dosyalar	Yürütülen dosya tarafından kaydedilen (oluşturulan veya değiştirilen) dosyaların bir listesi.
HTTPS/HTTP/DNS/IP/TCP/UDP vb.	Dosya yürütme/URL'de göz atma sırasında kaydedilen ağ oturumları/istek ayrıntıları.
Ağ trafiği dökümü (PCAP)	Ağ etkinliği, PCAP biçiminde dışarı aktarılabilir.
MITRE ATT&CK matrisi	Öykünme sırasında kaydedilen tüm tanımlanmış süreç faaliyetleri, bir MITRE ATT&CK matrisi biçiminde sunulur.

Kaspersky Threat Analysis

Kaspersky Threat Attribution Engine

Tehdit niteleme

Sürekli olarak gelişen BT güvenlik tehditlerinin takibi, analizi, yorumlanması ve azaltılması çok büyük bir girişimdir. Tehdit istihbaratı gerçek bir değer arz eder ve tehdit ilişkilendirme bu konu ile ilgili kritik bir unsurdur.

Bulut ve şirket içi sürümleri mevcuttur.

İlişkilendirme

Kaspersky Threat Attribution Engine, yüksek profilli kötü amaçlı yazılımların kaynağı ve olası yazarları hakkında derinlemesine bilgi sağlayan benzersiz bir tehdit analiz aracıdır. Benzersiz bir algoritma ve APT kötü amaçlı yazılım örnekleri ile Kaspersky uzmanları tarafından son 25 yılda toplanan sektörün en büyük temiz dosya koleksiyonunu içeren özel bir veritabanı kullanarak şüpheli bir dosyayı bilinen APT tehditlerine, aktörlerine, kampanyalarına hızlı bir şekilde bağlar.

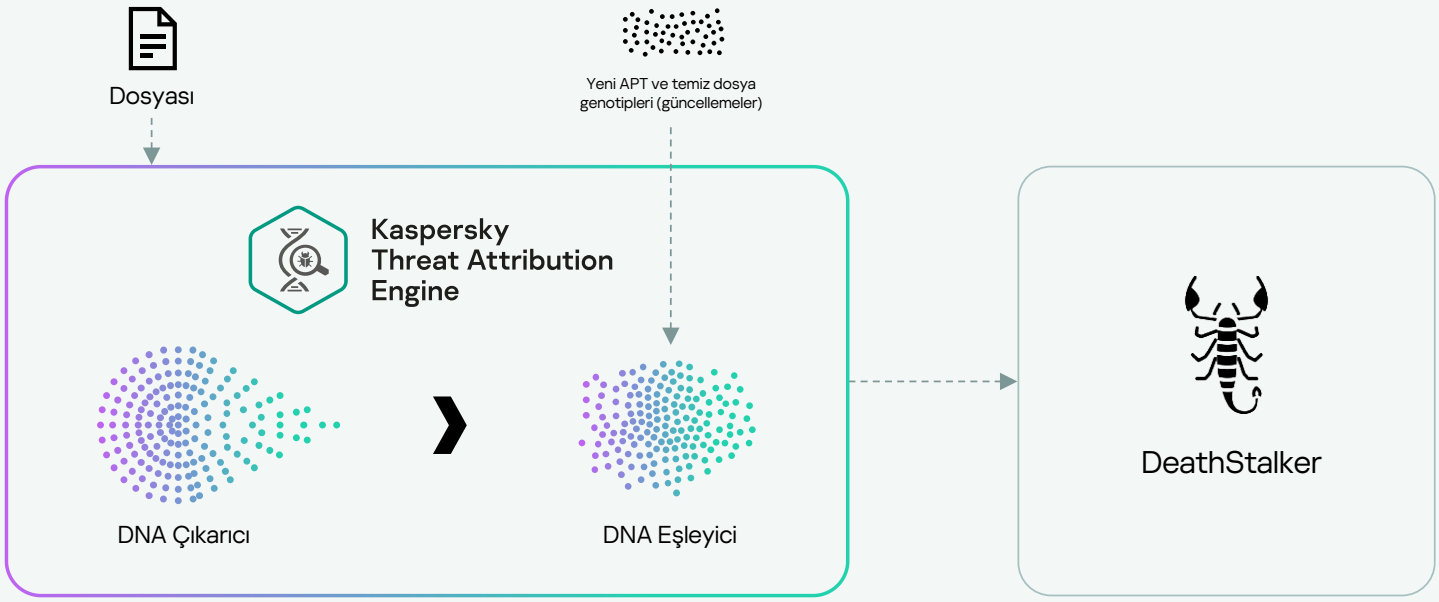
1100'den fazla tehdit aktörünü ve saldırılarını takip ediyor ve yılda 200'den fazla tehdit istihbarat raporu yayınlıyoruz. Sürmekte olan araştırmalarımız 80.000'den fazla dosya içeren bir APT koleksiyonunu desteklemekte ve otomatik araçların kullanımıyla birlikte olağanüstü doğrulukta ilişkilendirme seviyeleri elde edilmektedir.

Ürün, sıfıra yakın yanlış pozitif oranları sağlarken, benzer numuneleri karşılaştırmak için de benzersiz bir yaklaşım sunar. Herhangi bir yeni saldırı, bilinen APT kötü amaçlı yazılımları, önceki hedefli saldırılar ve bilgisayar korsanı grupları ile hızlı bir şekilde ilişkilendirilebilir, bu da yüksek riskli tehditleri daha az ciddi olaylardan ayırt etmenize yardımcı olur. Böylece bir saldırganın sisteminizde bir yer edinmesini önlemek için zamanında koruyucu önlemler alabilirsiniz. Kaspersky Threat Attribution Engine, 3. tarafların işlenmiş bilgilere ve gönderilen tehdit unsurlara erişimini önlemek için güvenli ve ayrı ortamlarda kurulabilir.

Neden kullanılmalı?

Bir dosyanın belirli bir tehdit aktörüne atfedilmesi, bu tehdit aktörünün bilgisi ile birlikte, bu örneğin genel siber ölüm zincirindeki yerini, bu düşmana özgü olarak bilmeyi sağlar. Bu da diğer IoC'lerin/IoA'ların nerede aranacağı bilgisini verir ve sadece belirli bir dosyayı engelleyerek tüm saldırıyı gözden kaçırmaz.

Kaspersky Threat Attribution Engine yüksek seviyeli operasyon şeması



Ürünün öne çıkan özellikleri

Binlerce APT aktörü, örneği ve daha geniş tehditler hakkında derlenmiş veri havuzuna anında erişim sağlar (anti-virüs motoru aracılığıyla)

Kaspersky uzmanları tarafından incelenen yüksek profilli kampanyalara (400+) ilişkin benzersiz bilgiler

Verimli bir otomatik veya manuel tehdit önceliklendirme ve uyarı saptaması sağlar

Özel aktörler ve nesneler ekleme ve ürünü özel koleksiyonunuzdaki dosyalara benzer örnekleri algılamak üzere eğitme işlevi

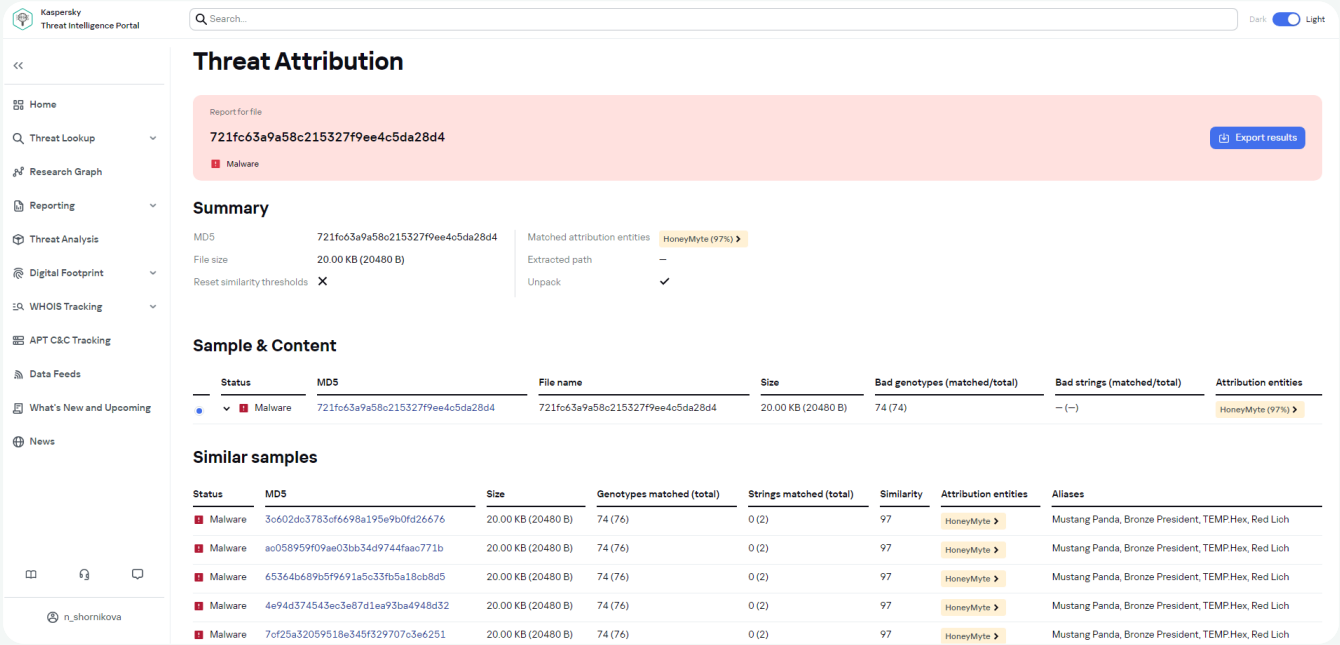
Manuel örnek yükleme ve otomatik iş akışlarıyla entegrasyon için geliştirilmiş REST API

Amazon Web Services (AWS) gibi bulut altyapılarında dağıtımı destekleyerek hızlı ürün kurulumu sağlar ve önceden donanım yatırımı yapmaya gerek olmadığından maliyet tasarrufu sağlar

Benzer dosyalar için daha fazla otomatik arama/tarama veya üçüncü taraf çözümlerle entegrasyon için YARA kurallarına aktarma yapın

Güvenlik günlüklerinin daha fazla otomatik analizi veya üçüncü taraf çözümleri/güvenlik kontrolleri ile entegrasyon için STIX 2.1 biçimine aktarma yapın (TXT ve JSON biçimleri de desteklenir)

Parola korumalı arşivleri özel parolalarla açmak için işlevsellik



Tescilli arama yöntemi

Kaspersky Threat Attribution Engine, kötü amaçlı yazılımları ilişkilendirme varlıklarına bağlamak için dosyalar arasında benzer genotipleri ve dizeleri aramak için benzersiz bir tescilli yöntem kullanır. Bu yöntem şunları içermektedir:

Kodundan aşağıdaki unsurları çıkararak

bir örneğin genetiğini analiz etme:

- Genotipler — ikili kodun ayırt edici parçaları
- Dizeler — ayırt edici karakter dizeleri

Analiz edilen dosyalarda,

daha önce analiz edilen APT örneklerinin genotiplerine ve dizelerine benzeyen veya zaten ilişkilendirilmiş varlıklarla bağlantılı olan genotiplerin ve dizelerin otomatik olarak aranması.

APT örneklerinde bulunan benzer

genotiplere ve dizelere dayanarak, analiz edilen örneğin kökeni, ilişkilendirilen varlıklar ve bu örnek ile bilinen APT örnekleri arasındaki benzerlikler hakkında bir rapor sunar.

Kaspersky Threat Analysis

Kaspersky Similarity

Dosya benzerliği

Etkili bir savunma hattı oluşturmak için düşmanınızı her zaman görerek tanımanız gerekmez. Kaspersky Similarity, bilinmeyen ve kaçamak tehditlere karşı koruma sağlamak için benzer işlevlere sahip dosya örneklerini tanımlamaya olanak tanır.

Bulut sürümü Kaspersky Threat Intelligence Portal üzerinden kullanılabilir.

Benzerlik

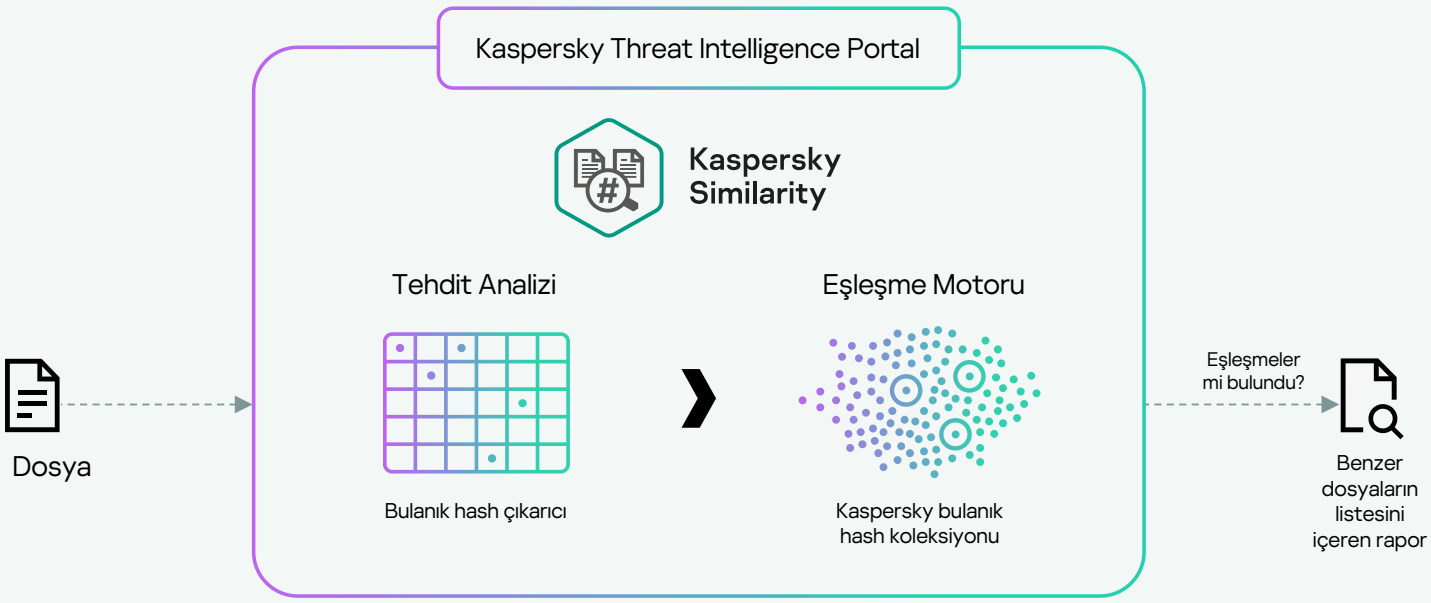
Kaspersky Similarity, hem Kaspersky Research Sandbox hem de Kaspersky Threat Attribution Engine kullanıcıları için Threat Intelligence Portal üzerinden kullanılabilen ve benzer şekilde görünen ve davranan dosyaları tanımlamaya yardımcı olan ek bir özelliktir.

Benzer dosyalar, Kaspersky uzmanları tarafından icat edilen ve 50'den fazla benzersiz benzerlik karması türünden yararlanan en son teknoloji kullanılarak orijinal dosya için aranır ve hesaplanır. Bu, doğru ve yüksek güvenilirlikte benzerlik sonuçları elde edilmesini sağlar.

Neden kullanılmalı?

Benzer (örneğin kaçamak) kötü amaçlı yazılımları bulun ve örnekte düşman tarafından yapılan küçük bir değişikliğin hala güvenlik radarınızda olduğundan emin olmak için altyapınızda arama yapın. Teknoloji ilişkilendirmeden farklıdır: ilişkilendirilmemiş benzer kötü amaçlı yazılım dosyaları bile bulunabilir.

Kaspersky Similarity üst düzey çalışma şeması



Benzerlik raporları

Her dosyanın kendine özgü biçimi, kullandığı paketleyicileri, bölümleri, dizeleri, içe aktarma tabloları vb. vardır. Kaspersky uzmanları, bu özniteliklere dayanarak farklı dosyalar arasındaki benzerlikleri belirlemek için bir dizi karma oluşturdu. Kaspersky Similarity, kullanıcıların şüpheli bir dosya göndermesine, bulanık karmalarını çıkarmasına ve bunları Kaspersky tehdit veritabanında bulunan dosyaların bulanık karmalarıyla karşılaştırmasına olanak tanır. Eşleşmelerin bulunması durumunda, Kaspersky tarafından zaten bilinen ve benzerlik puanına göre sıralanan TOP benzer kötü amaçlı dosyalar için karma listesi oluşturur. Rapor, her benzer dosya için meta verilerle birlikte ek bağlam içerir:

- Benzerlik güveni
- Dosya durumu (kötü amaçlı yazılım, reklam yazılımı veya diğer)
- Tehdit adı
- İlk ve son tespitin zaman damgaları
- İsabet sayısı (tespitler)
- Dosya karması
- Dosya türü
- Dosya boyutu

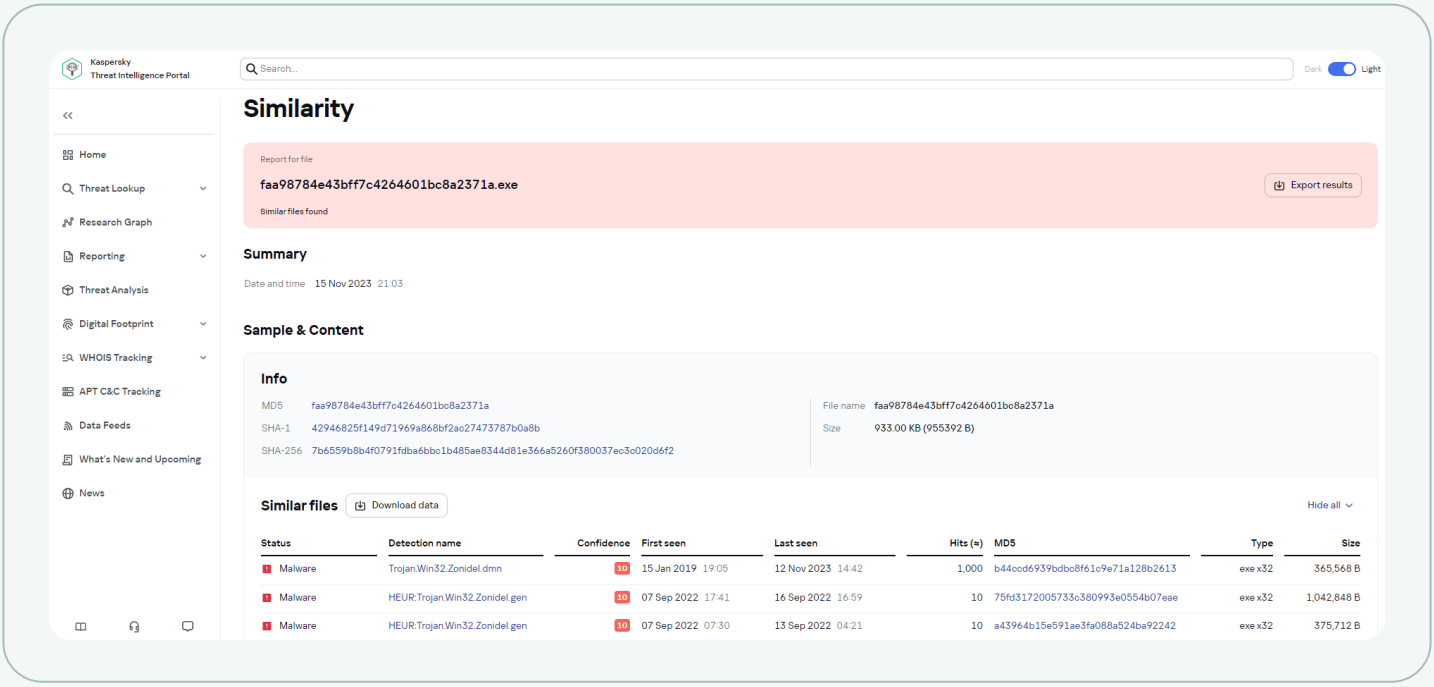
Öne çıkan özellikler

En yüksek karşılaştırma doğruluğu için maksimum kapsam sağlayan, 25 yıldan uzun süredir toplanmakta olan kötü amaçlı ve temiz dosyalardan oluşan sektördeki en büyük veritabanlarından birini kullanır

Manuel örnek yükleme ve otomatik iş akışlarıyla entegrasyon için geliştirilmiş REST API

Her iki teknolojinin etkinliğini artırmak ve analiz edilen dosya hakkında kapsamlı bilgi sağlamak için Kaspersky Research Sandbox ve Kaspersky Threat Attribution kullanıcılarına ücretsiz olarak sağlanır

Kaspersky uzmanları tarafından, bağımsız testler tarafından düzenli olarak en yüksek oranlarla onaylanan ürünlerimizde daha da yüksek tehdit koruması sağlamak amacıyla yeni tehditleri keşfetmek için zaten kapsamlı bir şekilde kullanılmaktadır:



Kaspersky Tehdit Analizi kullanım örnekleri

Kaspersky Tehdit Analizi bilinmeyen tehditleri tespit etmek için tercih edilen olgun araçlar sunar ve şu senaryolarda yaygın olarak uygulanabilir:

Olay Müdahalesi

Gizlenmeye çalışan tehditleri açığa çıkarma

Şüpheli dosyaların statik/dinamik analizi

Saldırının olası diğer adımlarını bilmek için yeni bir kötü amaçlı yazılımın belirli Tehdit Aktörü ile ilişkisini ortaya çıkarma

Tehdit Avlama

Rapor aracılığıyla alınan IoC'ler için altyapı taraması

Popüler temiz dosyaların olası kötü amaçlı modifikasyonlarını bulun

Bilinmeyen ve bilinen kötü amaçlı dosyalar arasında paylaşılan IoC'leri belirleyin

Kötü Amaçlı Yazılım Analizi

Bilinmeyen tehdit analizi

Gizlenmiş dosyalarda tersine mühendisliğe yardımcı olmak için ilgili kötü amaçlı yazılımları bulun

Kaspersky Tehdit Analizi, gelişmiş saldırıların tanımlanması ve sınıflandırılması için şüpheli nesnelerin kapsamlı ve çok katmanlı bir şekilde değerlendirilmesini sağlayan, birbirine bağlı bileşenlere sahip esnek bir araştırma aracıdır. SOC ekiplerinin, güvenlik araştırmacılarının ve kötü amaçlı yazılım analistlerinin var olan ve yeni ortaya çıkan kötü amaçlı yazılımlarla ilgili tehditler hakkında bilgi sahibi olmalarına yardımcı olarak kritik tehditleri hızlı bir şekilde önceliklendirmelerine, ele almalarına ve daha etkili bir şekilde düzeltmelerine olanak tanır.

Kaspersky Threat Analysis

Daha fazla bilgi edinin

www.kaspersky.com.tr

#kaspersky
#geleceğiyakalayın