kaspersky GELECEĞİ YAKALAYIN

Kaspersky Threat Attribution Engine

Sürekli olarak gelişen BT güvenlik tehditlerinin takibi, analizi, yorumlanması ve azaltılması çok büyük bir girişimdir. Tehdit istihbaratı, bilgi güvenliği endüstrisindeki gelişmekte olan mali fırsatlar balonunun ötesinde, gerçek bir değer taşıyor. Tehdit niteleme ise tehdit istihbaratı söz konusu olduğunda, muhtemelen en önemli ilgi odağı ve tartışma konusu.

Ürünün öne çıkan özellikleri:

- Yüzlerce APT aktörü ve örneğiyle ilgili düzenlenen verileri içeren bir depoya anında erişim sunar
- 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 API açma
- Her uyumluluk gereksinimini karşılamanın yanı sıra, sistemlerinizi ve verilerinizi korumak için güvenli ve ayrı ortamlarda dağıtılabilir
- Hassas bilgilerin ifşa edilmesini önlemek üzere tüm gönderimler için tam gizlilik sağlar

Bu, nedensiz bir durum değildir. Karışık sorgulama ve ters mühendislik süreçlerinden dolayı son derece sofistike tehditleri algılamadan müdahaleye kadar geçen ortalama süre genelde çok uzundur. Birçok durumda bu saldırganların amaçlarına ulaşması için yeterlidir. Doğru ve zamanında niteleme, hem olaya müdahale sürelerini saatlerden dakikalara kısaltmaya yardımcı olur hem de hatalı pozitif sonuçların sayısını azaltır.

Hedefli saldırıları tanımlamak, saldırganların profillerini çıkarmak ve farklı tehdit aktörleri için niteleme faktörleri oluşturma, uzun ve kapsamlı bir iştir ve yıllar sürebilir. Ayrıca, çalışan niteleme faktörleri oluşturmak için hem yıllar içerisinde birikmiş yüksek miktardaki verinin işlenmesi hem de soruşturmada tecrübeli, becerikli bir araştırma ekibi gerekir. Genel olarak araştırmacılar, farklı grupların etkinliklerini izler ve bilgi parçalarıyla veritabanını doldurur. Bu veri tabanı, araç olarak paylaşılabilen önemli bir kaynak haline gelir.

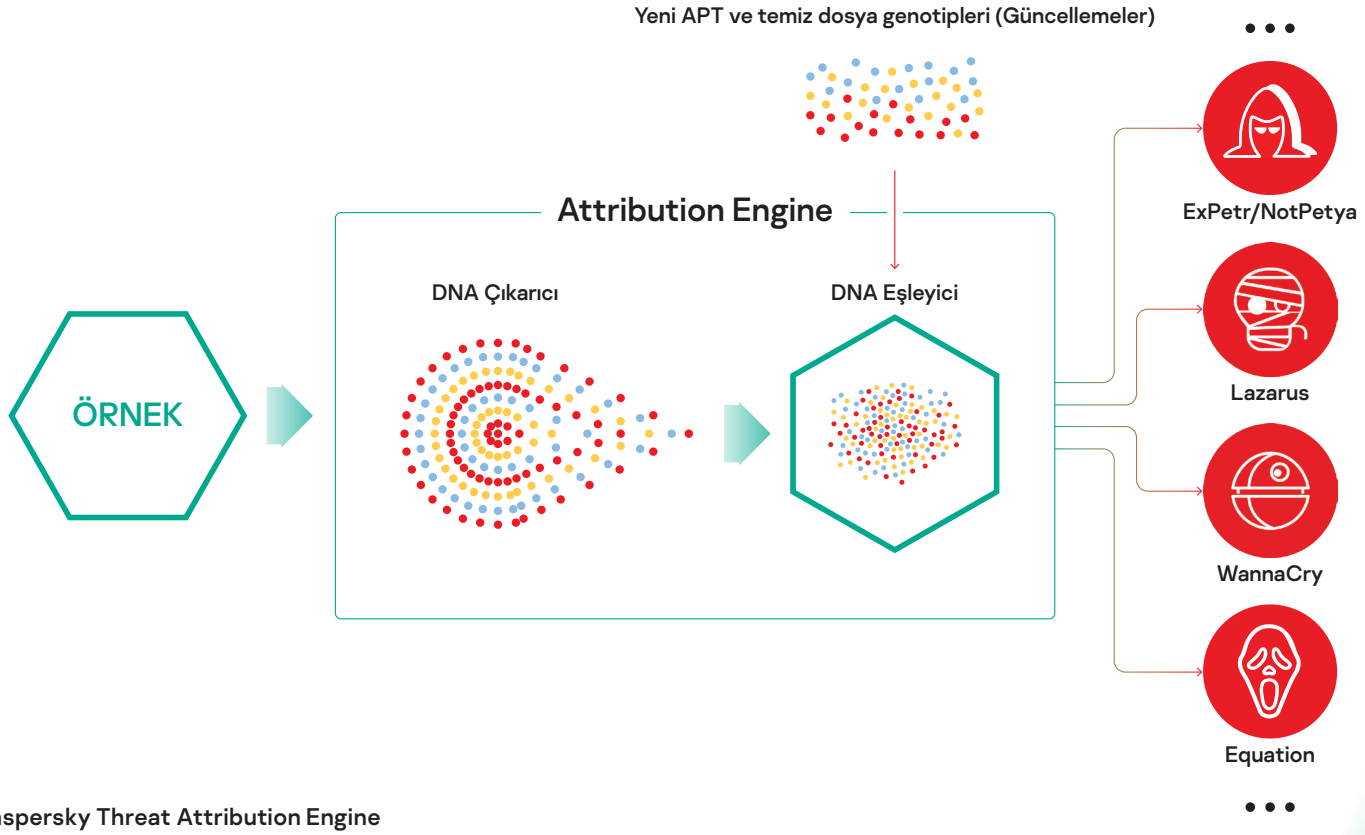
Kaspersky Threat Attribution Engine, APT kötü amaçlı yazılım örneklerinden oluşan bir veri tabanıyla Kaspersky uzmanlarının son 22 yıldır topladığı temiz dosyaları birleştirir. Her yıl yayınlanan 120'den fazla APT İstihbarat raporu ile 600'den fazla tehdit aktörü ve kampanyasını takip ediyoruz. Devam eden araştırmamız, 60.000'den fazla dosya içeren büyük APT koleksiyonumuzun güncel kalmasına yardım ediyor. Bu durum, yanlış alarm algılamasını iyileştiriyor ve otomatik araçlar kullanarak niteleme işlemini olabildiğince doğru hale getiriyor.

Bu ürün, örnekleri benzerlik yönünden karşılaştırmaya benzersiz bir yaklaşım sunar ve sıfır hatalı pozitif sonuç oranları sunar. Daha az ciddi olaylardaki yüksek riskli tehdidi görmenize yardımcı olarak ve saldırganın sisteme erişim fırsatı elde edememesi için zamanında koruyucu önlemler alarak, yeni bir saldırıyı hızlıca bilindik APT kötü amaçlı yazılımıyla, önceki hedefli saldırılarla ve korsan gruplarıyla ilişkilendirebilir.

Nasıl çalışır?

Kaspersky Threat Attribution Engine, kötü amaçlı yazılımların "genetiğini" inceleyerek otomatik olarak, bağlantılı aktörler ve daha öncesoruşturulmuş olan APT örnekleriyle kod benzerliği arar. Bu ürün, "genotipleri" yani ayrıştırılmış dosyaların ufak ikili parçalarını, APT kötü amaçlı yazılım örnekleri veritabanıyla karşılaştırır ve kötü amaçlı yazılımın kaynağına, tehdit aktörlerine ve bilinen APT örnekleriyle dosya benzerliğine dair bir rapor sunar.Ayrıca ürün, güvenlik ekibinin üründeki veritabanına özel aktörler ve nesneler eklemesine ve ürünü, özel koleksiyonunuzdaki dosyalara benzer örnekleri algılamak üzere eğitmesine olanak tanır. Threat Attribution Engine sayesinde niteleme işlemi, geçmişteki gibi yıllarca sürmez ve saniyeler içerisinde tamamlanır.

Bu ürün, 3. tarafların işlenmiş bilgilere ve gönderilen nesnelere erişmesini önlemek için güvenli ve ayrı ortamlarda dağıtılabilir. Nitelemeyi, mevcut altyapıya ve otomatik işlemlere uygulamak amacıyla Engine'i diğer araç ve çerçevelere eklemek için bir API arayüzü bulunmaktadır.



Kaspersky Threat Attribution Engine

İlgili APT aktörleri hakkında detaylı bilgiler, Kaspersky APT İstihbarat raporlarında[1] bulunabilir. Kaspersky APT İstihbarat Raporlaması abonesi olarak size, ortaya çıkarılan her APT ile ilgili, asla kamuya açıklanmayacak tehditler de dahil olmak üzere çeşitli biçimlerde sağlanan eksiksiz teknik veriler dahil, çeşitli incelemelerimiz ve keşiflerimize eşsiz bir sürekli erişim sunuyoruz.

Kaspersky Threat Attribution Engine, ulusal siber güvenlik kurumlarını ve ticari Güvenlik Operasyonu Merkezlerini (SOC'ler), etkili bir olay yönetimi süreci oluşturma konusunda destekleyerek, bu kuruluşlara yönelik Kaspersky portföyünü daha da genişletir ve güçlendirir.

Kaspersky Attribution Engine, güvenlik operasyonlarını önemli ölçüde iyileştirerek şu konularda yardımcı olur:

- Siber olayların arkasındaki amaçları, yöntemleri ve araçları ortaya çıkarmak için dosyaları hızlıca, bilinen APT aktörleriyle ilişkilendirme;
- Doğru önleme ve yanıt prosedürleri oluşturmak amacıyla bir saldırının hedefi veya ikincil kurbanı olup olmadığınızı hızlıca değerlendirme;
- Kaspersky APT İstihbarat Raporlaması'nda sunulan, APT ailesine dair eyleme geçirilebilir tehdit istihbaratına uygun şekilde, etkili ve zamanında tehdit hafifletme işlemleri uygulama.

1 Kaspersky APT İstihbaratı'na abonelik Raporlama ayrı olarak satın alınmalıdır

Siber Tehdit Haberleri: www.securelist.com
BT Güvenliği Haberleri: business.kaspersky.com
KOBİ'ler için BT Güvenliği: kaspersky.com.tr/business
Kurumlar için BT Güvenliği: kaspersky.com.tr/enterprise

www.kaspersky.com

Kanıtlanmış başarılara sahibiz. Bağımsızız. Şeffafız. Teknolojinin hayatlarımızı geliştirdiği, daha güvenli bir dünya oluşturmakta kararlıyız. Teknolojiyi, ortaya çıkardığı sonsuz sayıdaki fırsattan herkes yararlanabilsin diye daha güvenli hale getiriyoruz. Daha güvenli bir gelecek için siber güvenliğe önem verin.

Daha fazla bilgi için: kaspersky.com.tr/transparency

Proven.
Transparent.
Independent.