Kaspersky Research Sandbox

kaspersky GELECEĞİ YAKALAYIN

Korumalı alan teknolojileri

Korumalı alan teknolojileri; dosya örneği kaynaklarının araştırılmasına, davranış analizine dayalı IOC'lerin toplanmasına ve daha önce görülmemiş kötü amaçlı nesnelerin tespit edilmesine olanak sağlayan güçlü araçlardır.

Kaspersky Research Sandbox

Bir dosyanın veya URL'nin davranışına dayalı akıllı bir karar verirken eş zamanlı olarak işlem belleğini, ağ etkinliğini vb. analiz etmek, güncel karmaşık hedefli ve özel tehditlerini anlamak için en iyi yaklaşımdır.

Günümüzdeki kötü amaçlı yazılımlar, kötü amaçlı etkinliğinin açığa çıkmasına neden olabilecekse kodunu yürütmemek için çeşitli yöntemler kullanır. Sistem gerekli parametreleri karşılamıyorsa kötü amaçlı program hemen hemen her zaman kendini yok edecek ve hiçbir iz bırakmayacaktır. Bu sebeple kötü amaçlı kodun yürütülebilmesi için korumalı alanın normal son kullanıcı davranışını doğru bir şekilde taklit edebilmesi gerekir.

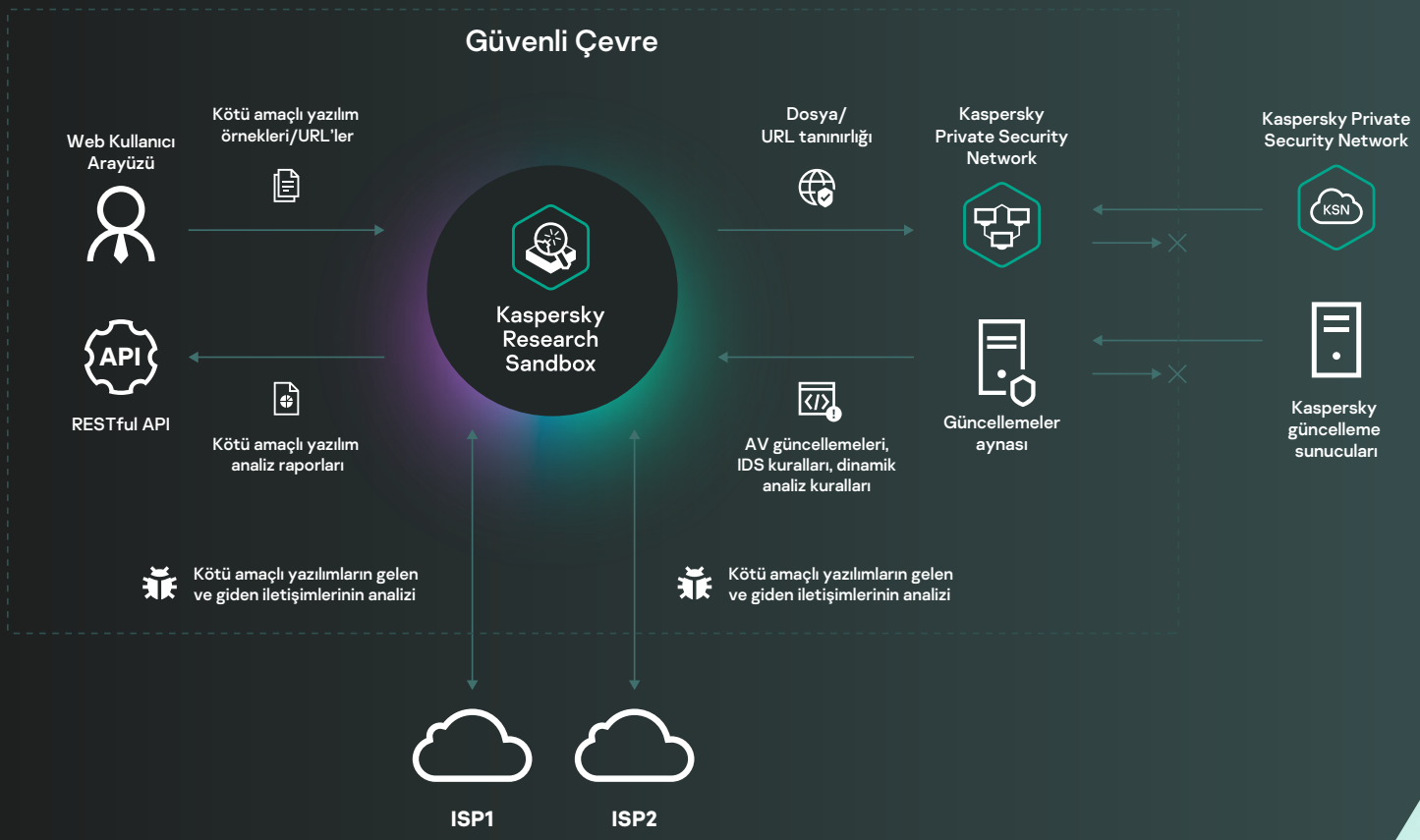
Kaspersky Research Sandbox, doğrudan on yıldan fazla bir süredir gelişen bir teknoloji olan laboratuvar kullanımına yönelik korumalı alan kompleksimizden geliştirilmiştir. Kesintisiz tehdit araştırmalarımız boyunca edindiğimiz kötü amaçlı yazılım davranışları hakkındaki tüm bilgileri bir araya getirirken aynı zamanda her gün 380.000'den fazla yeni kötü amaçlı nesneyi tespit etmemizi sağlar. Bu güçlü teknoloji, yerinde kullanıldığında verilerin kuruluş dışında açığa çıkarılmasını da önler.

Davranış analizini ve son derece sağlam atlatma önleme tekniklerini insan simülasyonu teknolojileriyle birleştiren hibrit bir yaklaşım sunar. Kaspersky Research Sandbox, aynı zamanda sistem görüntülerinin analiz amaçlı özelleştirilmesine olanak sağlarken bu görüntüleri gerçek ortamlara göre uyarlar; böylece tehdit algılamanın doğruluğunu ve araştırmanın hızını artırır.

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
- Yerinde dağıtım sayesinde kuruluş dışında hiçbir verinin açığa çıkmaması sağlanır
- Gelişmiş atlatma karşıtı teknikler ve insan simülasyonlu teknolojiler
- Manuel dosya/URL gönderimi ve RESTful API
- Ayrıntılı analiz raporlarıyla 100'den fazla dosya türünün analizi için destek
- Ağ trafiğini taramak için özel Suricata kuralları eklenebilir ve kullanıma hazır olarak sunulan Suricata kurallarıyla birlikte kullanılabilir
- Ürün, işletim sistemi/yazılım içermeyen dağıtımı destekler ve gerekli performansa bağlı olarak kolayca ölçeklenebilir

Kaspersky Research Sandbox yüksek seviyeli mimarisi



Ürün, işletim sistemi/yazılım içermeyen dağıtımı destekler. Donanım yapılandırması, gerekli performansa bağlıdır ve ölçeklenebilir. Her kanal için 100 Mb/sn. ağ bağlantısı ve en az bir bağımsız İSS bağlantısı gerekir (hata toleransı için iki veya daha fazlası önerilir). İSS, kötü niyetli trafiklere karşı farkında ve hazır olmalıdır.

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.

Kötü amaçlı yazılımlar, korumalı alanda eksik olan belirli bir uygulamayı hedef alıyorsa kötü amaçlı davranışını göstermeyebilir. Araştırmacılar, bu sorunu gidermek için günlükleri incelemeli, eksikleri anlamalı, eksik olan şeyleri sanal bir makineye eklemeli ve bu işlemi tekrar çalıştırmalıdırlar. Kötü amaçlı yazılım bir uygulamaya erişmeye çalıştığında patentli sistem bu girişimi engeller. Kötü amaçlı yazılım, dosya yürütme tamamlanana kadar beklemez; bunun yerine gerekli uygulamayı ve içeriği oluşturma işlemini duraklatır.

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 Research Sandbox, bilinmeyen tehditleri tespit etmek için tercih edilen araçtır. Diğer tüm çözümlere göre daha köklüdür ve gelişmiş tehditlere daha fazla odaklanır.

www.kaspersky.com.tr