kaspersky geleceği yakalayın

Kaspersky
Threat Intelligence

# Kaspersky Threat Data Feeds

# Genel Bakış

## Akışlarda ne var

Kaspersky tarafından sağlanan veri akışlarındaki girdiler, tehditleri hızlı bir şekilde onaylamanızı ve önceliklendirmenizi sağlayan bağlamsal veriler içerir:

- tehdit adları
- belirlenen kötü amaçlı web kaynaklarının IP adresleri ve domain'leri
- kötü amaçlı dosya grupları
- savunmasız ve güvenliği ihlal edilmiş öğelerin tanımlayıcıları
- MITRE ATT&CK sınıflandırmasına göre hazırlanmış saldırı taktikleri, teknikleri ve prosedürleri
- zaman damgaları
- coğrafi konum
- bilinirlik ve daha fazlası.

Kaspersky Threat Data Feeds hizmeti, kuruluşların ağlarını ve sistemlerini siber tehditlere karşı korumalarına yardımcı olmak için gerçek zamanlı tehdit istihbaratı bilgileri sunar. Veri akışları, bilinen kötü amaçlı yazılımlar, kimlik avı siteleri, en son güvenlik açıkları ve sömürüleri ile diğer siber tehdit türleri hakkında bilgiler içerir. Şirketler bu bilgileri kötü amaçlı trafiği engellemek, güvenlik yazılımlarını güncellemek ve kendilerini siber saldırılardan korumak üzere gerekli önlemleri almak için kullanabilir.

Veriler, Kaspersky Security Network ve kendi tarayıcılarımız, botnet tehdit izleme hizmeti (7/24 botnet izleme, hedefleri ve etkinlikleri), spam tuzakları, araştırma gruplarından ve iş ortaklarından gelen veriler dâhil olmak üzere çok çeşitli güvenilir kaynaklardan toplanır.

Toplanan tüm bilgiler, çeşitli ön işleme yöntemleri kullanılarak gerçek zamanlı olarak dikkatlice kontrol edilir ve temizlenir. Söz konusu ön işleme yöntemleri arasında korumalı alanda test etme (sandboxing), istatistiksel ve sezgisel analiz, benzerlik araçları, davranış profili oluşturma ve uzman analizleri bulunur.

Veri Akışları, bir etkinlik hakkında genel bilgi toplamaya ve ayrıntılara inmeye yardımcı olur. Ayrıca şu soruları yanıtlayabilmenize de yardımcı olur: 'Kim? Ne? Nerede? Neden?' Böylece, bir saldırının kaynağını belirleyebilmenizi sağlayarak şirketinizi her türlü karmaşıklıktaki tehditlerden korumak için hızlı karar vermenizi mümkün kılar.

## Veri akışları nasıl kullanılır?

| Akış adı | Önleme | Algılama | Araştırma |
|---|---|---|---|
| Kötü amaçlı URL Veri Akışı | • | • | • |
| Fidye Yazılımı URL Veri Akışı | • | • | • |
| Kimlik Avı URL'si Veri Mesajı | • | • | • |
| Botnet C&C URL Veri Akışı | • | • | • |
| Mobil Botnet C&C URL Veri Akışı | • | • | • |
| Kötü Amaçlı Karma Veri Akışı | • | • | • |
| Mobil Kötü Amaçlı Karma Veri Akışı | • | • | • |
| IP İtibarı Veri Akışı | • | • | • |
| IoT URL Veri Akışı | • | • | • |
| Zayıf Nokta Veri Akışı | • | • | • |
| ICS Güvenlik Açığı Veri Akışı | • | • | • |
| OVAL formatta ICS Güvenlik Açığı Veri Akışı | | • | |
| ICS Karma Veri Akışı | • | • | • |
| pDNS Veri Akışı | | | • |

| Akış adı | Önleme | Algılama | Araştırma |
|---|---|---|---|
| Suricata Kuralları Veri Akışı | | • | |
| Cloud Access Security Broker (CASB) Veri Akışı | | • | |
| APT Karma Veri Akışı | | • | • |
| APT IP Veri Akışı | | • | • |
| APT URL Veri Akışı | | • | • |
| APT Yara Veri Akışı | | • | • |
| Açık Kaynaklı Yazılım Tehditleri Veri Akışı | • | • | • |
| Suç Amaçlı Yazılım Karma Veri Akışı | | • | • |
| Suç Amaçlı Yazılım URL Veri Akışı | | | • |
| Suç Amaçlı Yazılım Yara Veri Akışı | | | • |
| Sigma Kuralları Veri Akışı | • | | |
| Ağ Güvenliği IP Veri Akışı | • | • | |
| Ağ Güvenliği URL Veri Akışı | • | • | |
| Ağ Güvenliği Web Filtreleme Veri Akışı | • | • | |

Kaspersky Threat Data Feeds listesi sürekli genişliyor.

# Kaspersky Threat Data Feeds Açıklaması

## Ticari akışlar

Ticari akışlar, abonelik yoluyla elde edilebilecek en kapsamlı bilgi koleksiyonuna erişim sağlar. Bilgiler düzenli olarak güncellenir. Akışın türüne bağlı olarak, güncellemelerin düzenliliği birkaç dakika ile birkaç saat arasında değişebilir. Listelenen veri akışlarına ek olarak, ihtiyaçlarınıza göre özel bir akış oluşturmayı talep edebilirsiniz.

| Akış adı | Akış açıklaması | Gösterge türü | Kullanım senaryoları |
|---|---|---|---|
| Kötü amaçlı URL Veri Akışı | Kötü amaçlı yazılımların dağıtıldığı web kaynakları | Maske | • Bilgi güvenliği yönetim sistemleri dış bilgi kaynakları ile zenginleştirilmeye açıktır. Bu akışların SIEM / SOAR / IRP'ye bağlanması, kullanıcıların mevcut tehditlere zamanında yanıt vermesine ve bir olayı araştırırken ek bağlam oluşturmasına olanak tanır.<br>• Ağ ve e-posta güvenlik sistemleri (örneğin, NGFW/ IDS/IPS/Mail/Web Güvenliği) ile entegrasyon, yerel güvenlik kontrol yeteneklerini veri akışından gelen IOC'lerle zenginleştirerek siber olayların önlenmesine yardımcı olur. |
| Fidye Yazılımı URL Veri Akışı | Fidye yazılımının dağıtıldığı web kaynakları | | |
| Kimlik Avı URL'si Veri Mesajı | Kimlik avı web kaynakları | | |
| Botnet C&C URL Veri Akışı | Botnet C&C sunucuları ve ilgili kötü amaçlı nesneler (botlar) | | |
| Mobil Botnet C&C URL Veri Akışı | İlişkili kötü amaçlı nesneler (botlar) ile C&C mobil botnet sunucuları | | |

#Önleme

#Algılama

#İnceleme

| Akış adı | Akış açıklaması | Gösterge türü | Kullanım senaryoları | |
|---|---|---|---|---|
| Kötü Amaçlı Karma Veri Akışı | Yaygın kötü amaçlı dosya grupları | Hash | • Kötü amaçlı yazılımların indirilmesini ve çalıştırılmasını önlemek ve halihazırda çalışan kötü amaçlı yazılımları tespit etmek için altyapı güvenlik sistemleriyle (Uç Nokta Güvenliği, Sunucu Güvenliği, Posta/Web Güvenliği) entegrasyon.<br>• SIEM / SOAR / IRP sistemleri ile entegrasyon, kullanıcıların mevcut tehditlere hızlı bir şekilde yanıt vermesine ve bir olayı araştırırken ek bağlam oluşturmasına olanak tanır. | #Önleme<br>#Algılama<br>#İnceleme |
| Mobil Kötü Amaçlı Karma Veri Akışı | Mobil işletim sistemleri (Android ve iOS) için yaygın zararlı dosya grupları | | | |
| IP İtibarı Veri Akışı | Şüpheli ve kötü niyetli IP adreslerinin çeşitli kategorileri | IP | • Ağ ve posta güvenlik sistemleri (NGFW / Posta Güvenliği) ile entegrasyon, mevcut tehditlerle ilgili verilerle uzlaşma göstergelerinin yerel veritabanını tamamlayarak siber olayların önlenmesine yardımcı olur.<br>• SIEM/SOAR/IRP sınıfı sistemlerle entegrasyon, kullanıcıların mevcut tehditlere hızlı bir şekilde yanıt vermesine ve bir olayı araştırırken ek bağlam oluşturmasına olanak tanır. | #Önleme<br>#Algılama<br>#İnceleme |
| IoT URL Veri Akışı | IoT cihazları (IP kameralar, akıllı elektrikli süpürgeler, çaydanlıklar, kahve makineleri vb.) için kötü amaçlı yazılım dağıtan web kaynakları | Maske | | |
| Zayıf Nokta Veri Akışı | Kurumsal yazılım güvenlik açıkları | CVE | • Güvenlik açığı tarayıcıları ve Varlık Yönetimi sistemleri ile entegrasyon yoluyla hassas altyapı unsurlarının belirlenmesi.<br>• Kritik güvenlik açıkları içeren yazılımların piyasaya sürülmesini önlemek üzere Uç Nokta Koruma sistemleri ile entegrasyon.<br>• Savunmasız yazılımın başlatıldığının tespiti.<br>• Soruşturmalarda yardım.<br>• Güvenlik açıklarının azaltılması için öneriler. | #Önleme<br>#Algılama<br>#İnceleme |
| ICS Güvenlik Açığı Veri Akışı | ICS yazılım ve donanımının yanı sıra süreç kontrol altyapısında kullanılan kurumsal yazılımlardaki güvenlik açıkları | | | |

| Akış adı | Akış açıklaması | Gösterge türü | Kullanım senaryoları | |
|---|---|---|---|---|
| OVAL formatta ICS Güvenlik Açığı Veri Akışı | ICS yazılım güvenlik açıkları için otomatik arama kuralları | OVAL kontrolü | • Güvenlik açığı olan ICS yazılımlarını tespit etmek için popüler yazılım güvenlik açığı tarayıcılarının zenginleştirilmesi. | #Algılama |
| ICS Karma Veri Akışı | ICS için tehdit oluşturan yaygın kötü amaçlı dosyalar | Hash | • Kötü Amaçlı Karma Veri Akışlarını kullanma senaryolarına benzer şekilde OT ağlarının çevresinde.<br>• Potansiyel olarak tehlikeli dosyaları algılamak için OT ağlarının içinde. | #Önleme<br>#Algılama<br>#İnceleme |
| pDNS Veri Akışı | Belirli bir süre boyunca alan adlarına karşılık gelen IP adresleri için DNS aramalarının kayıtları | IP, FQDN | • Siber olayları araştırırken bağlam sağlanması | #İnceleme |
| Suricata Kuralları Veri Akışı | Ağ trafiğindeki APT, Botnet C&C, Fidye Yazılımı vb. gibi çeşitli tehdit kategorilerini tespit etmek için kurallar. | Suricata kuralı | • Kötü niyetli faaliyetlerin tespitine yönelik kuralları zenginleştirmek için NGFW/IDS/IPS/NTA/NDR sistemleri ile entegrasyon. | #Algılama |
| Cloud Access Security Broker (CASB) Veri Akışı | Popüler bulut hizmetleriyle ilgili alan adları ve ana bilgisayarlar | Maske | • Özellikle bulut hizmetleri için erişim politikaları oluşturmak üzere bir CASB çözümü oluşturulması. | #Algılama |

| Akış adı | Akış açıklaması | Gösterge türü | Kullanım senaryoları | |
|---|---|---|---|---|
| APT Karma Veri Akışı | APT çeteleri tarafından hedefli saldırılar gerçekleştirmek için kullanılan dosya karmaları | Hash | • Kötü amaçlı yazılımların indirilmesini ve çalıştırılmasını önlemek ve halihazırda çalışan kötü amaçlı yazılımları algılamak için altyapı güvenlik sistemleriyle (Uç Nokta ve Sunucu Güvenliği) entegrasyon.<br>• Ağ ve e-posta güvenlik sistemleri (örneğin, NGFW/ IDS/IPS/Mail/Web Güvenliği) ile entegrasyon, yerel güvenlik kontrol yeteneklerini veri akışından gelen IOC'lerle zenginleştirerek siber olayların önlenmesine yardımcı olur.<br>• SIEM / SOAR / IRP sınıfı sistemlerle entegrasyon, kullanıcıların bir olayı araştırırken ek bağlam oluşturmasına ve hedefli saldırılarla ilgili veya APT gruplarının üyeleriyle ilgili mevcut tehditlere zamanında yanıt vermesine olanak tanır. | #Algılama<br>#İnceleme |
| APT IP Veri Akışı | Hedefli saldırıların gerçekleştirilmesiyle ilgili altyapı unsurları hakkında bilgiler | IP | | |
| APT URL Veri Akışı | | Maske | | |
| APT Yara Veri Akışı | Hedefli saldırılarda kullanılan dosyaları tanımlamak için YARA kuralları | YARA kuralı | • Bir kuruluşun altyapısındaki hedefli saldırıların işaretleri için proaktif arama.<br>• Siber olayları araştırırken kullanışlıdır. | #Algılama<br>#İnceleme |
| Açık Kaynaklı Yazılım Tehditleri Veri Akışı | Güvenlik açıkları, kötü niyetli işlevsellik veya siyasi amaçlı işlevsellik ihlalleri (belirli bölgelerde engellemeler, siyasi sloganlar, vb.) içeren açık kaynaklı yazılım paketleri | Paket adı ve sürümü | • Yazılımı tedarik zinciri saldırılarından korumak, güvenlik açıklarını erken tespit etmek ve ortadan kaldırmak ve ayrıca siyasi odaklı bildirilmemiş özellikler (NDV) içeren paketlerin kullanımını önlemek için güvenli geliştirme sürecinin (DevSecOps) bir parçası olarak geliştirilen yazılımın bileşen analizi için tasarlanmıştır. | #Önleme<br>#Algılama<br>#İnceleme |

| Akış adı | Akış açıklaması | Gösterge türü | Kullanım senaryoları | |
|---|---|---|---|---|
| Suç Amaçlı Yazılım Karma Veri Akışı | Kaspersky Crimeware raporlarında tanımlanan dolandırıcılık kampanyalarında kullanılan dosya karmaları | Hash | • Davetsiz misafirlerin dolandırıcılık eylemleriyle ilişkili kötü niyetli faaliyetlerin algılanması.<br>• Tehdit veri akışlarında bulunan ek bilgilerin sağlanması yoluyla olay çözümüne yardımcı olunması. | #Algılama<br>#İnceleme |
| Suç Amaçlı Yazılım URL Veri Akışı | Kaspersky Crimeware raporlarında açıklanan dolandırıcılık kampanyalarıyla ilgili altyapı unsurları hakkında bilgiler | Maske | | |
| Suç Amaçlı Yazılım Yara Veri Akışı | Kaspersky Crimeware raporlarında açıklanan dolandırıcılık kampanyalarında kullanılan dosyaları tanımlamak için YARA kuralları | YARA kuralı | • Kurumun altyapısında dolandırıcılık kampanyalarının işaretlerini proaktif olarak arayın.<br>• Siber olayları araştırırken kullanışlıdır. | #İnceleme |
| Sigma Kuralları Veri Akışı | Kötü niyetli faaliyetleri tespit etmek için YAML formatında kurallar | SIGMA kuralları | • Kötü niyetli faaliyetleri algılamak için SIEM/EDR ile entegrasyon | #Algılama |
| Ağ Güvenliği IP Veri Akışı | NGFW uyarı/red listeleri için IP adresleri listesi | IP | • Koruma seviyelerini artırmak için ağ güvenlik kontrolleri (NGFW'ler) ile entegrasyon | #Algılama<br>#Önleme |

| Akış adı | Akış açıklaması | Gösterge türü | Kullanım senaryoları | |
|---|---|---|---|---|
| Ağ Güvenliği URL Veri Akışı | NGFW uyarı/red listeleri için URL'lerin listesi | URL | • Koruma seviyelerini artırmak için ağ güvenlik kontrolleri (NGFW'ler) ile entegrasyon | #Algılama<br>#Önleme |
| Ağ Güvenliği Web Filtreleme Veri Akışı | NGFW uyarı/red listeleri için kategorize edilmiş alan adlarının listesi | URL | • Koruma seviyelerini artırmak için ağ güvenlik kontrolleri (NGFW'ler) ile entegrasyon | #Algılama<br>#Önleme |

## Demo akışlar

Demo akışlar yalnızca değerlendirme amaçlıdır. Veriler, önemli ölçüde azaltılmış bilgilere ve daha az sıklıkta güncellemelere sahip sınırlı örnekler içermektedir. Akışların yapısı ticari akışların formatına benzer, ancak bu bazı durumlarda farklılık gösterebilir.

Demo IP İtibarı Veri Akışı

Demo Botnet C&C URL Veri Akışı

Demo Kötü Amaçlı Karma Veri Akışı

Demo APT IP Veri Akışı

Demo APT URL Veri Akışı

Demo Sigma Kuralları Veri Akışı

Demo APT Karma Veri Akışı

Demo Suricata Kuralları Veri Akışı

Demo Suricata Kuralları Veri Akışı

Demo ICS Güvenlik Açığı Veri Akışı

Demo OVAL formatta ICS Güvenlik Açığı Veri Akışı

Demo Suç Amaçlı Yazılım Karma Veri Akışı

Demo Suç Amaçlı Yazılım URL Veri Akışı

Demo talep edin

# Kaspersky Threat Intelligence

## Zengin destekleyici bağlamınız

Kaspersky tarafından sunulan Threat Data Feeds çözümü; SIEM sistemleri, izinsiz giriş algılama sistemleri, güvenlik proxy'leri vb. dahil olmak üzere mevcut güvenlik kontrollerinizin algılama özelliklerini geliştirir.

Daha fazla bilgi edinin

www.kaspersky.com.tr