kaspersky bring on the future

Kaspersky
Threat Intelligence

Kaspersky Thread Data Feeds

Overzicht

Wat er in de feeds staat

Vermeldingen in feeds van Kaspersky, bevatten contextuele gegevens waarmee je dreigingen snel kunt bevestigen en prioriteren:

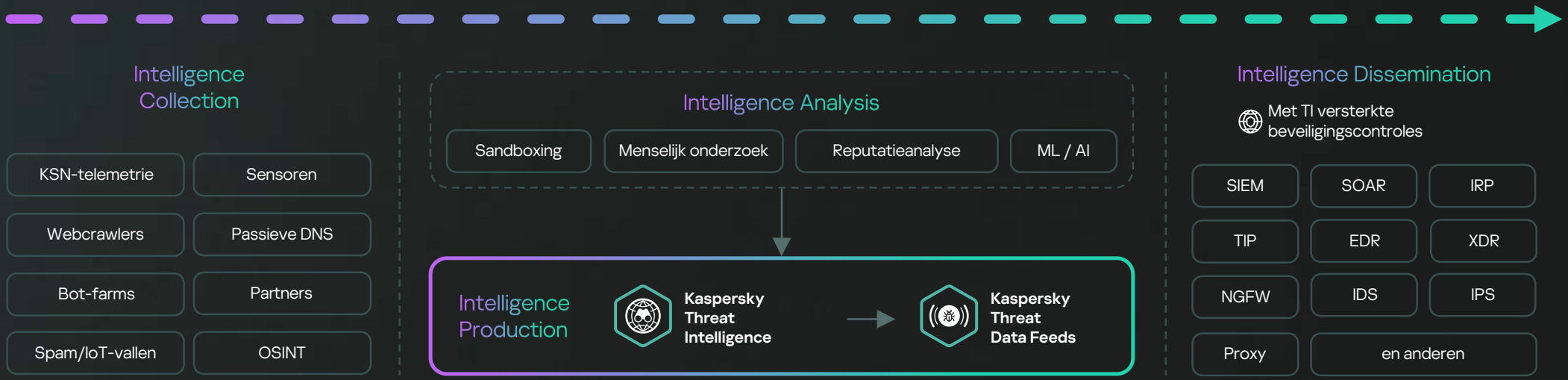
- namen van dreigingen
- IP-adressen en domeinnamen van vastgestelde schadelijke webbronnen
- hashes van schadelijke bestanden
- id's van kwetsbare en gehackte objecten
- tactieken, technieken en procedures van aanvallen volgens de classificatie MITRE ATT&CK
- tijdstempels
- geografische ligging
- populariteit, enzovoort.

De service van Kaspersky Threat Data Feed geeft in real time informatie over dreigingen om organisaties te helpen hun netwerken en systemen te beschermen tegen cyberdreigingen. De gegevensfeeds bevatten informatie over bekende malware, phishingwebsites, de laatste kwetsbaarheden en exploits en andere typen cyberbedreigingen. Organisaties kunnen aan de hand van deze informatie schadelijk internetverkeer blokkeren, hun beveiligingssoftware bijwerken en maatregelen nemen ter bescherming tegen cyberaanvallen.

De gegevens worden verzameld uit een breed scala aan betrouwbare bronnen, waaronder Kaspersky Security Network en onze eigen crawlers, services voor het monitoren van botnetdreigingen (botnets en hun doelwitten en activiteiten worden de klok rond gevolgd), spamtraps, gegevens van onderzoeksgroepen en partners.

Alle informatie die is verzameld, wordt in real time zorgvuldig gecontroleerd en opgeschoond met verschillende methoden voor voorverwerking: sandboxen, statistische en heuristische analyse, tools voor gelijkenissen, gedragsprofilering en deskundige analyse.

Met gegevensfeeds kun je algemene informatie over een gebeurtenis te verzamelen en zo in details duiken. Ze helpen ook antwoord te geven op de vragen "Wie? Wat? Waar? Waarom?" en de bron van een aanval te identificeren, waardoor je snel beslissingen kunt nemen en je bedrijf kunt beschermen tegen dreigingen, hoe complex dan ook.



Zo gebruik je gegevensfeeds

Naam van feed	Preventie	Detectie	Onderzoek
Gegevensfeed voor schadelijke URL's	•	•	•
Gegevensfeed voor ransomware-URL's	•	•	•
Phishing URL Data Feed	•	•	•
Gegevensfeed voor Botnet C&C-URL's	•	•	•
Gegevensfeed voor mobiele Botnet C&C-URL's	•	•	•
Gegevensfeed voor schadelijke hashes	•	•	•
Gegevensfeed voor mobiele schadelijke hashes	•	•	•
Gegevensfeed voor IP-reputaties	•	•	•
Gegevensfeed voor IoT-URL's	•	•	•
Gegevensfeed voor kwetsbaarheden	•	•	•
Gegevensfeed voor ICS-kwetsbaarheden	•	•	•
Gegevensfeed voor ICS-kwetsbaarheden (in OVAL-indeling)		•	
Gegevensfeed voor ICS-hashes	•	•	•
Gegevensfeed voor pDNS			•

Naam van feed	Preventie	Detectie	Onderzoek
Gegevensfeed voor Suricata-regels		•	
Gegevensfeed voor Cloud Access Security Brokers (CASB)		•	
Gegevensfeed voor APT-hashes		•	•
Gegevensfeed voor APT-IP's		•	•
Gegevensfeed voor APT-URL's		•	•
Gegevensfeed voor APT-YARA		•	•
Feed met dreigingsgegevens van Open Source Software	•	•	•
Gegevensfeed voor crimewarehashes		•	•
Gegevensfeed voor crimeware-URL's			•
Feed met gegevens over crimeware-YARA			•
Gegevensfeed voor Sigma-regels	•		
Gegevensfeed voor netwerkbeveiligings-IP's	•	•	
Gegevensfeed voor netwerkbeveiligings-URL's	•	•	
Gegevensfeed voor webfilters voor netwerkbeveiliging	•	•	

De lijst van Kaspersky-feeds met dreigingsgegevens wordt steeds langer.

Beschrijving van Kaspersky-feeds met dreigingsgegevens

Commerciële feeds

Met commerciële feeds krijg je toegang tot de meest uitgebreide informatie, afhankelijk van het abonnement. De informatie in deze feeds wordt regelmatig bijgewerkt. Hoe vaak dit gebeurt, hangt af van het type feed. De updatefrequentie kan variëren van enkele minuten tot enkele uren. Naast de benoemde gegevensfeeds, kun je ook vragen om zelf een gepersonaliseerde feed te maken.

Naam van feed	Beschrijving van informatiefeed	Type indicator	Gebruiksscenario's
Gegevensfeed voor schadelijke URL's	Webresources waarvan de malware afkomstig is	Masker	• Beheersystemen voor informatiebeveiliging worden gebruikt voor het verkrijgen van externe informatiebronnen. Door deze stromen te verbinden met SIEM, SOAR of IRP, kunnen gebruikers op tijd reageren op huidige dreigingen en voor extra context zorgen wanneer ze een incident onderzoeken. • Door integratie met beveiligingssystemen voor netwerken en e-mailprogramma's (bijvoorbeeld NGFW, IDS, IPS, Mail of Web Security), kun je cyberincidenten voorkomen door native functies voor beveiligingscontroles te gebruiken met IoC's vanuit gevensfeeds.
Gegevensfeed voor ransomware-URL's	Webresources waarvan de ransomware afkomstig is		
Phishing URL Data Feed	Phishing-webresources		
Gegevensfeed voor Botnet C&C-URL's	Botnet C&C-servers en gerelateerde schadelijke objecten (bots)		
Gegevensfeed voor mobiele Botnet C&C-URL's	Mobiele Botnet C&C-servers met gerelateerde schadelijke objecten (bots)		

#Preventie

#Detectie

#Onderzoek

Naam van feed	Beschrijving van informatiefeed	Type indicator	Gebruiksscenario's	
Gegevensfeed voor schadelijke hashes	Hashes van veelvoorkomende schadelijke bestanden	Hash	• De integratie met beveiligingssystemen voor de infrastructuur (Endpoint Security, Server Security, Mail/Web Security) om te voorkomen dat malware wordt gedownload en uitgevoerd, alsook om reeds aanwezige malware te detecteren. • Door de integratie met SIEM-, SOAR- of IRP-systemen kunnen gebruikers snel reageren op huidige dreigingen en voor extra context zorgen wanneer ze een incident onderzoeken.	#Preventie #Detectie #Onderzoek
Gegevensfeed voor mobiele schadelijke hashes	Hashes van veelvoorkomende schadelijke bestanden voor mobiele besturingssystemen (Android en iOS)			
Gegevensfeed voor IP-reputaties	Verschillende categorieën van verdachte en schadelijke IP-adressen	IP	• Door integratie met beveiligingssystemen voor netwerken en e-mailprogramma's (NGFW of Mail Security) kun je cyberincidenten voorkomen door de native database te voorzien van IoC's met gegevens over huidige dreigingen. • Door de integratie met SIEM-, SOAR- of IRP-klassensystemen kunnen gebruikers snel reageren op huidige dreigingen en voor extra context zorgen wanneer ze een incident onderzoeken.	#Preventie #Detectie #Onderzoek
Gegevensfeed voor IoT-URL's	Webresources waarmee schadelijke software wordt verspreidt voor IoT-apparaten (IP-camera's, slimme stofzuigers, waterkokers, koffiezetapparaten, enz.)	Masker		
Gegevensfeed voor kwetsbaarheden	Kwetsbaarheden in software van bedrijven	CVE	• Identificatie van kwetsbare onderdelen in een infrastructuur door de integratie met kwetsbaarheidscanners en assetbeheersystemen. • De integratie met systemen voor endpointbescherming om te voorkomen dat software met kritische kwetsbaarheden wordt uitgevoerd. • Detectie van het uitvoeren van kwetsbare software. • Begeleiding bij onderzoeken. • Aanbevelingen voor het beperken van kwetsbaarheden.	#Preventie #Detectie #Onderzoek
Gegevensfeed voor ICS-kwetsbaarheden	Kwetsbaarheden in ICS-software en -hardware, alsook de bedrijfssoftware die is gebruikt voor de infrastructuur in het procesbeheer			

Naam van feed	Beschrijving van informatiefeed	Type indicator	Gebruiksscenario's	
Gegevensfeed voor ICS-kwetsbaarheden (in OVAL-indeling)	Regels voor geautomatiseerde zoekopdrachten voor ICS-softwarekwetsbaarheden	OVAL-controle	• Het gebruik van populaire scanners voor softwarekwetsbaarheden om kwetsbare ICS-software te detecteren.	#Detectie
Gegevensfeed voor ICS-hashes	Veelvoorkomende schadelijke bestanden die een dreiging vormen voor ICS	Hash	• Bij de perimeter van OT-netwerken, vergelijkbaar met de redenen voor het gebruik van de gegevensfeed voor schadelijke hashes. • Binnen OT-netwerken om mogelijk gevaarlijke bestanden te detecteren.	#Preventie #Detectie #Onderzoek
Gegevensfeed voor pDNS	Records van DNS-zoekopdrachten gedurende een bepaalde periode voor domeinen met overeenkomende IP-adressen	IP, FQDN	• Context bieden bij het onderzoeken van cyberincidenten	#Onderzoek
Gegevensfeed voor Suricata-regels	Regels voor het detecteren van verschillende soorten dreigingen in het netwerkverkeer, zoals APT, Botnet C&C, ransomware, enz.	Suricata-regel	• Integratie met NGFW-, IDS-, IPS-, NTA- of NDR-systemen voor meer regels waarmee schadelijke activiteiten kunnen worden gedetecteerd.	#Detectie
Gegevensfeed voor Cloud Access Security Brokers (CASB)	Domeinen en hosts die zijn gerelateerd aan populaire cloudservices	Masker	• Voor het maken van een CASB-oplossing om een toegangsbeleid voor cloudservices op te stellen.	#Detectie

Naam van feed	Beschrijving van informatiefeed	Type indicator	Gebruiksscenario's	
Gegevensfeed voor APT-hashes	Hashes van bestanden die zijn gebruikt door APT-bendes om doelgerichte aanvallen uit te voeren	Hash	• De integratie met beveiligingssystemen voor de infrastructuur (Endpoint Security of Server Security) om te voorkomen dat malware wordt gedownload en uitgevoerd, alsook om reeds aanwezige malware te detecteren. • Door integratie met beveiligingssystemen voor netwerken en e-mailprogramma's (bijvoorbeeld NGFW, IDS, IPS, Mail of Web Security), kun je cyberincidenten voorkomen door native functies voor beveiligingscontroles te gebruiken met IoC's vanuit gevensfeeds. • Door de integratie met SIEM-, SOAR- of IRP-systemen kunnen gebruikers voor extra context zorgen wanneer ze een incident onderzoeken. Ook kunnen gebruikers op tijd reageren op huidige dreigingen die zijn gerelateerd aan doelgerichte aanvallen of leden van APT-bendes.	#Detectie #Onderzoek
Gegevensfeed voor APT-IP's	Relevante gegevens over onderdelen binnen een infrastructuur voor het uitvoeren van doelgerichte aanvallen	IP		
Gegevensfeed voor APT-URL's		Masker		
Gegevensfeed voor APT-YARA	YARA-regels voor het identificeren van bestanden die zijn gebruikt in doelgerichte aanvallen	YARA-regel	• Proactief zoeken naar tekenen van doelgerichte aanvallen op de infrastructuur van een organisatie. • Handig bij het onderzoeken van cyberincidenten.	#Detectie #Onderzoek
Feed met dreigingsgegevens van Open Source Software	Pakketten voor opensourcesoftware met kwetsbaarheden, schadelijke functies of functies die zijn gehackt uit politieke motiveringen (blokkeringen in bepaalde regio's, politieke slogans, enz.)	Naam en versie van pakket	• Ontworpen voor het analyseren van componenten in ontwikkelde software als onderdeel van het ontwikkelingsproces voor de veiligheid (DevSecOps). Zo kan software worden beschermd tegen supply chain-aanvallen, kunnen kwetsbaarheden al vroeg worden gedetecteerd en verholpen en kan het gebruik worden voorkomen van pakketten met politiek georiënteerde functies die niet zijn aangegeven (NDV).	#Preventie #Detectie #Onderzoek

Naam van feed	Beschrijving van informatiefeed	Type indicator	Gebruiksscenario's	
Gegevensfeed voor crimewarehashes	Hashes van gebruikte bestanden in frauduleuze campagnes die zijn benoemd in Kaspersky Crimeware-rapporten	Hash	• Detectie van schadelijke activiteiten die zijn gerelateerd aan frauduleuze acties van aanvallers. • Helpen bij het oplossen van een incident door aanvullende informatie te geven uit feeds met dreigingsgegevens.	#Detectie #Onderzoek
Gegevensfeed voor crimeware-URL's	Informatie over onderdelen in de infrastructuur die zijn gerelateerd aan frauduleuze campagnes benoemd in Kaspersky Crimeware-rapporten	Masker		
Feed met gegevens over crimeware-YARA	YARA-regels voor het identificeren van gebruikte bestanden in frauduleuze campagnes die zijn benoemd in Kaspersky Crimeware-rapporten	YARA-regel	• Proactief zoeken naar tekenen van frauduleuze campagnes in de infrastructuur van de organisatie. • Handig bij het onderzoeken van cyberincidenten.	#Onderzoek
Gegevensfeed voor Sigma-regels	Regels in YAML-indeling voor het detecteren van schadelijke activiteiten	SIGMA-regels	• Integratie met SIEM of EDR voor het detecteren van schadelijke activiteiten	#Detectie
Gegevensfeed voor netwerkbeveiligings-IP's	Lijst van IP-adressen voor 'alert lists' of 'deny lists' van NGFW	IP	• Integratie met beveiligingscontroles voor netwerken (NGFW's) voor betere bescherming	#Detectie #Preventie

Naam van feed	Beschrijving van informatiefeed	Type indicator	Gebruiksscenario's	
Gegevensfeed voor netwerkbeveiligings-URL's	Lijst van URL's voor 'alert lists' of 'deny lists' van NGFW	URL	• Integratie met beveiligingscontroles voor netwerken (NGFW's) voor betere bescherming	#Detectie #Preventie
Gegevensfeed voor webfilters voor netwerkbeveiliging	Lijst van ingedeelde domeinen voor 'alert lists' of 'deny lists' van NGFW	URL	• Integratie met beveiligingscontroles voor netwerken (NGFW's) voor betere bescherming	#Detectie #Preventie

Demofeeds

De demofeeds zijn uitsluitend voor evaluatiedoeleinden. De gegevens bevatten beperkte voorbeelden met aanzienlijk minder gegevens en minder frequente updates.
De structuur van de feeds is vergelijkbaar met de indeling van commerciële feeds, maar de indeling kan per geval verschillen.

Demo van gegevensfeed voor IP-reputaties

Demo van gegevensfeed voor Botnet C&C-URL's

Demo van gegevensfeed voor schadelijke hashes

Demo van gegevensfeed voor APT-IP's

Demo van gegevensfeed voor APT-URL's

Demo van gegevensfeed voor Sigma-regels

Demo van gegevensfeed voor APT-hashes

Demo van gegevensfeed voor Suricata-regels

Demo van gegevensfeed voor Suricata-regels

Demo van gegevensfeed voor ICS-kwetsbaarheden

Demo van gegevensfeed voor ICS-kwetsbaarheden (in OVAL-indeling)

Demo van gegevensfeed voor crimewarehashes

Demo van gegevensfeed voor crimeware-URL's

Een demo aanvragen

Kaspersky Threat Intelligence

Jouw ondersteunende rijke context

Feeds met dreigingsgegevens van Kaspersky vergroten de detectiemogelijkheden van je bestaande beveiligingscontroles, waaronder SIEM-systemen, inbraakdetectiesystemen, beveiligingsproxy's, etc.

Meer informatie

www.kaspersky.nl