Kaspersky Onderzoekssandbox

Kaspersky Threat Attribution Engine

Kaspersky Similarity

Kaspersky Threat Analysis

kaspersky bring on the future

Kaspersky Threat Analysis

Kaspersky Threat Analysis

Als je te maken krijgt met een potentiële cyberbedreiging, is het van belang welke beslissingen je neemt en op welke manier je dat doet. Het is onmogelijk om de gerichte aanvallen van tegenwoordig te voorkomen met alleen anti-virustools. Anti-virus-engines kunnen alleen bekende dreigingen en variaties hierop stoppen. Tegelijkertijd doen geraffineerde aanvallers er alles aan om automatische detectie te omzeilen. Het aantal beveiligingsmeldingen dat Security Operations Centers (SOC's) dagelijks verwerken, groeit exponentieel. Nu het aantal vormen van malware iedere dag toeneemt, is het effectief prioriteren, herkennen en valideren van waarschuwingen bijna onuitvoerbaar.

De combinatie van bedreigingsintelligentie, dynamische analyse, bedreigingsattributie en gelijkenistechnologieën vormt een krachtige tool om schadelijke objecten te detecteren die voorheen onbekend waren. Kaspersky biedt een enkele veerkrachtige structuur om automatisch verdachte bestanden mee te analyseren, waardoor beveiligingsonderzoekers op de hoogte kunnen blijven van bestaande en opkomende bedreigingen.

Naast traditionele analysetechnologieën voor bedreigingen zoals sandboxing, beschermt Kaspersky Threat Analysis je met geavanceerde attributie en gerelateerde gelijkenistechnologieën. Deze hybride aanpak biedt efficiënte bedreigingsanalyse, zodat je goed geïnformeerde keuzes kunt maken en je infrastructuur veilig kunt houden.

Kaspersky Threat Analysis wordt via een verbonden web en RESTful-interfaces aangeboden en stelt gebruikers in staat om specifieke parameters in te stellen waarmee verdachte objecten zeer efficiënt kunnen worden geanalyseerd. Met een combinatie van meerdere tools voor bedreigingsanalyse kunnen jij en je team de situatie vanuit alle hoeken analyseren. Ook biedt het een complete en gedetailleerde rapportage om snel en effectief te kunnen reageren.

Hoe het werkt

Kaspersky
Threat Analysis

Kaspersky
Research
Sandbox

Sandboxtechnologieën

zijn krachtige tools voor dynamische analyse waarmee je de herkomst van bestanden kunt onderzoeken, IOC's kunt verzamelen op basis van gedragsanalyse en schadelijke objecten kunt identificeren die niet worden gedetecteerd door traditionele anti-virus-tools.

Lokale en cloudversies zijn beschikbaar.

Sandbox

Kaspersky Research Sandbox is een technologie die we direct vanuit ons sandbox-laboratorium al twee decennia aan het ontwikkelen zijn. Het omvat alle kennis over malwaregedrag die we hebben opgedaan tijdens ons voortdurende bedreigingsonderzoek, waardoor we elke dag meer dan 420.000 nieuwe schadelijke objecten kunnen detecteren. Het biedt een hybride aanpak, waarbij gedragsanalyse en solide anti-ontwijkingstechnieken worden gecombineerd met technologieën die menselijk gedrag simuleren.

Deze technologie wordt op locatie geïmplementeerd en voorkomt dat gegevens op straat komen te liggen. Met Kaspersky Research Sandbox kun je uitvoeringsomgevingen aanpassen aan echte omgevingen om de nauwkeurigheid van bedreigingsdetectie en snelheid van het onderzoek te verhogen.

Waarom zou je dit moeten gebruiken?

Verdachte bestanden die niet worden gedetecteerd door anti-virus-tools, vormen pas echt een gevaar als ze hun gedrag kunnen uitvoeren. Met Kaspersky Research Sandbox kan dit gedrag worden geëmuleerd en worden gevaarlijke acties aan het licht gebracht.

Belangrijke product kenmerken

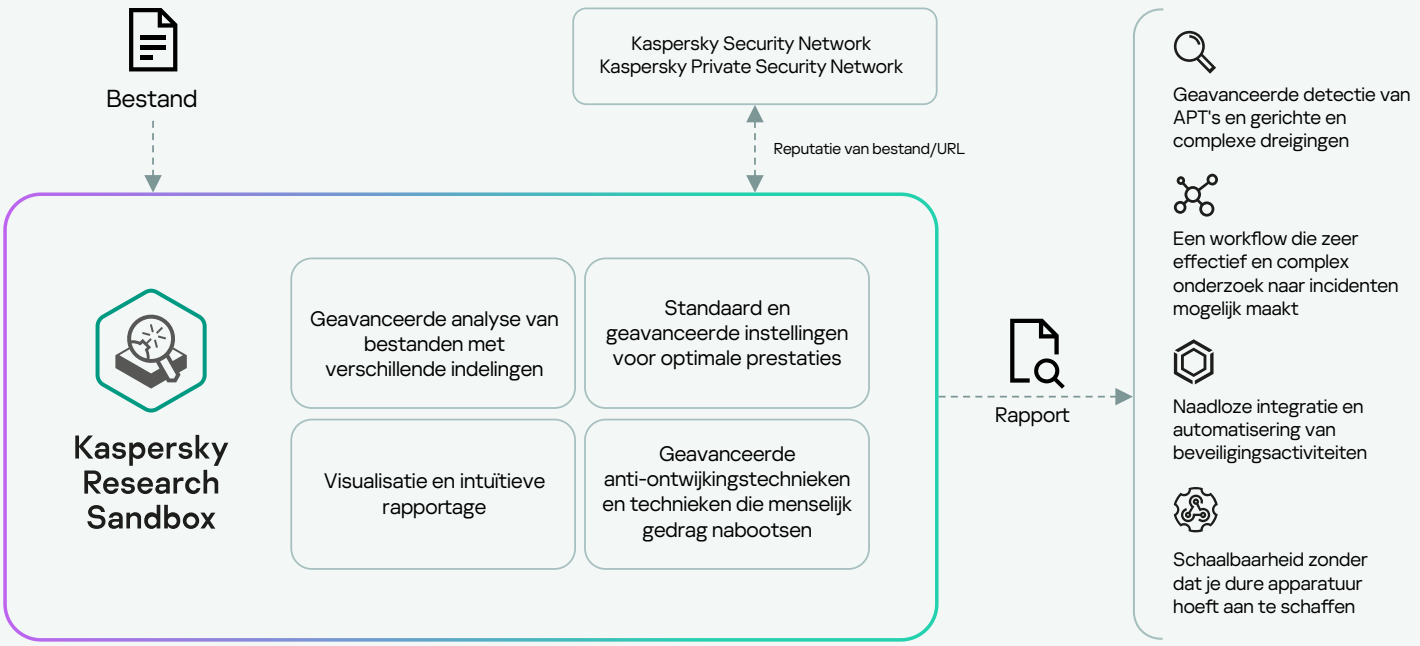
- Geautomatiseerde objectanalyse in Windows-, Linux- en Android-omgevingen
- Dreigingsdetectie binnen Windows-systemen en -applicaties dankzij aangepaste installatiekopieën (alleen als ze op echte omgevingen zijn gebaseerd)
- De bedreigingsscore op basis van statistieken en gegevens die worden verkregen tijdens het uitvoeren van een bestand, toont het risiconiveau van het geanalyseerde object
- Geavanceerde anti-ontwijkingstechnieken en technieken die menselijk gedrag nabootsen
- Handmatige upload van exemplaren en een geavanceerde REST API om te integreren met geautomatiseerde workflows
- Analyseondersteuning van ruim 200 bestandstypen met gedetailleerde analyserapporten
- Aangepaste Suricata-regels om netwerkverkeer te scannen, kunnen worden toegevoegd aan en samen met de Suricata-regels worden gebruikt
- Meer dan 1000 unieke opsporingen om TTP's uit te pakken door MITRE ATT&CK
- Support voor interactieve modus (verwacht in het eerste kwartaal van 2024)

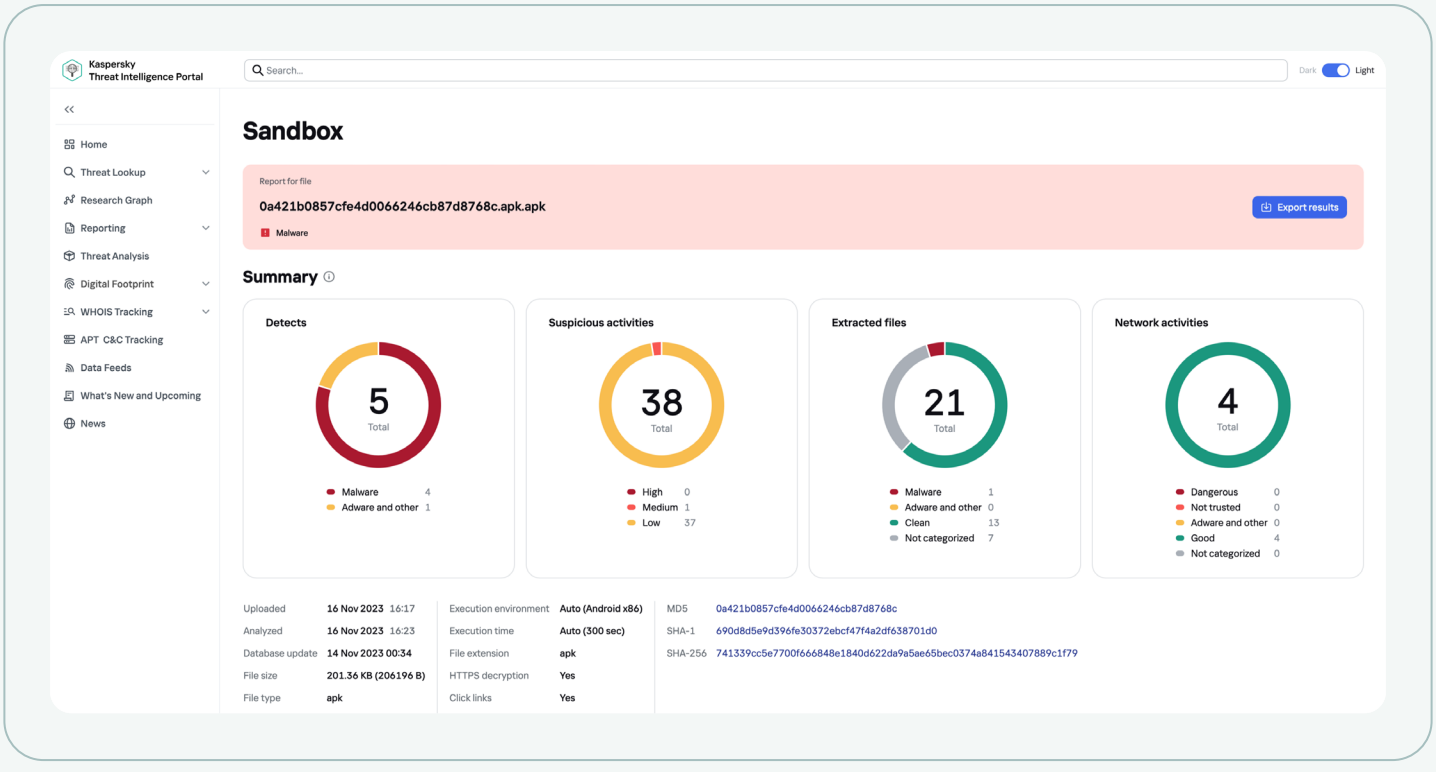
Het product ondersteunt bare-metal-implementatie. De hardwareconfiguratie is afhankelijk van de vereiste prestaties en kan opgeschaald worden. Er is tenminste één onafhankelijke ISP-verbinding vereist (twee of meer wordt aanbevolen in verband met fouttolerantie) met 100 Mbps voor elk kanaal.

Kaspersky Research Sandbox is gebaseerd op een gepatenteerde propriëtaire technologie (patentnummer US10339301). Door de precieze omstandigheden na te bootsen die het uitvoeren van malware triggeren, kunnen onderzoekers een verdacht bestand/verdachte URL in één keer analyseren.

Een kwaadaardig bestand kan, om blootstelling te voorkomen, eerst onderzoeken of het zich in een virtuele machine bevindt of kan inactief blijven tot de sandbox niet meer draait. In dergelijke gevallen versnelt de gepatenteerde technologie de tijd in de virtuele machine, zodat de schadelijke code eerder moet worden uitgevoerd.

Overkoepelend uitvoeringsschema van Kaspersky Research Sandbox





Gedetailleerde analyse rapporten

Als de analyse is voltooid, geeft de Onderzoekssandbox een gedetailleerd rapport over het gedrag en de functie van het geanalyseerde monster, waardoor jij de gewenste procedures kunt uitvoeren:

Samenvatting	Algemene informatie over het uitvoeren van een bestand/zoekresultaten van een URL.
Detectienamen	Een lijst van detecties (zowel AV en gedrag) die zijn geregistreerd tijdens het uitvoeren van het bestand.
Getriggerde netwerkregels	Een lijst van Suricata-netwerkregels die zijn getriggerd tijdens de analyse van het verkeer van het uitgevoerde object.
Uitvoermap	Een grafische reeksweergave van objectactiviteiten en de relatie ertussen.
Verdachte activiteiten	Verdachte activiteiten: een lijst met geregistreerde, verdachte activiteiten.
Schermafbeeldingen	Een reeks schermafbeeldingen die werden gemaakt tijdens het uitvoeren van het bestand/het navigeren door URL's.
Ingeladen PE-afbeeldingen	Een lijst van ingeladen PE-afbeeldingen die werden gedetecteerd tijdens het uitvoeren van bestanden/het navigeren door URL's.
Bestandsbewerkingen	Een lijst van bestandsbewerkingen die werden geregistreerd tijdens het uitvoeren van het bestand/het navigeren door URL's.
Registratiebewerkingen	Een lijst van bewerkingen die zijn uitgevoerd in het register van het besturingssysteem en zijn gedetecteerd tijdens het uitvoeren van het bestand/het navigeren door URL's.
Procesbewerkingen	Een lijst van bestandsinteracties met verschillende processen die zijn geregistreerd tijdens het uitvoeren van het bestand.
Synchronisatiebewerkingen	Een lijst met bewerkingen van aangemaakte synchronisatieobjecten (mutex, event, semaphore) die zijn geregistreerd tijdens het uitvoeren van het bestand/het navigeren door URL's.
Gedownloade bestanden	Een lijst van bestanden die werden geëxtraheerd uit het netwerkverkeer tijdens het uitvoeren van het bestand/het navigeren door URL's.
Opgeslagen bestanden	Een lijst van bestanden die zijn opgeslagen (aangemaakt of aangepast) door het uitgevoerde bestand.
HTTPS/HTTP/DNS/IP/TCP/UDP en meer.	Gegevens van netwerksessies/-verzoeken die werden opgenomen tijdens het uitvoeren van het bestand/het navigeren door URL's.
Dump van netwerkverkeer (PCAP)	Netwerkactiviteit kan in PCAP-formaat worden gedownload.
MITRE ATT&CK-matrix	Alle geïdentificeerde procesactiviteiten die tijdens de emulatie zijn opgenomen, worden weergegeven in de vorm van een MITRE ATT&CK-matrix.

Kaspersky
Threat Analysis

Kaspersky
Threat Attribution
Engine

Bedreigingsat-tributie

Het volgen, analyseren, interpreteren en inperken van de voortdurend veranderende IT-beveiligingsdreigingen is een enorme onderneming. Afgezien van alle hype is bedreigingsintelligentie erg belangrijk, waarbij bedreigingsattributie een kritische rol speelt.

Lokale en cloudversies zijn beschikbaar.

Attributie

Kaspersky Threat Attribution Engine is een unieke tool voor bedreigingsanalyse die inzicht biedt in de herkomst van bekende malware en mogelijke actoren. Het koppelt een verdacht bestand direct aan een bekende APT-bedreiging, actor of campagne door middel van een uniek algoritme en speciale database die exemplaren van APT-malware bevat en de grootste verzameling schone bestanden in de industrie. Deze bestanden zijn de afgelopen 25 jaar verzameld door experts van Kaspersky.

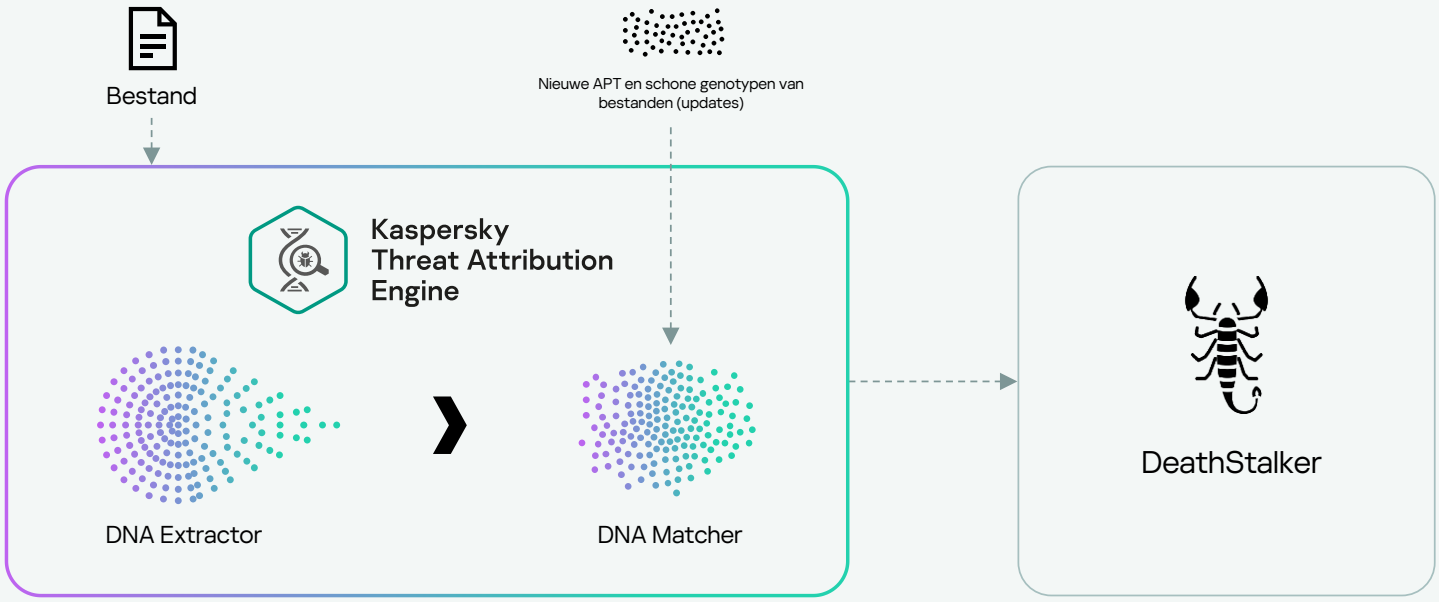
We houden meer dan 1100 bedreigingsactoren en campagnes bij en we leveren meer dan 200 bedreigingsintelligentierapporten per jaar. Ons voortdurende onderzoek ondersteunt een APT-collectie die meer dan 80.000 bestanden bevat en dat, samen met het gebruik van geautomatiseerde tools, voor ongekend precieze niveaus van attributie zorgt.

Het product biedt een unieke aanpak voor het vergelijken van soortgelijke bestanden met een zeer lage kans op fout-positieve resultaten. Een nieuwe aanval kan snel worden gekoppeld aan bekende APT-malware, gerichte aanvallen uit het verleden en hackergroepen, waardoor je bedreigingen met een hoog risico kunt onderscheiden van minder gevaarlijke incidenten. Op deze manier kun je op tijd beschermingsmaatregelen nemen om er voor te zorgen dat een aanvaller geen grip krijgt op je systeem. Kaspersky Threat Attribution Engine kan worden geïmplementeerd in beveiligde, geïsoleerde omgevingen, waardoor externe partijen geen toegang hebben tot de verwerkte gegevens en ingediende objecten.

Waarom zou je dit moeten gebruiken?

De attributie van een bestand aan een bepaalde bedreigingsactor, in combinatie met de kennis van deze bedreigingsactor, zorgt ervoor dat we de plaats van dit exemplaar kunnen herkennen in de algemene cyber kill chain, die typisch is voor deze aanvaller. Het geeft daarnaast ook aan waar je andere IoC's en IoA's kunt vinden en zorgt ervoor dat je de gehele aanval niet over het hoofd ziet door één bepaald bestand te blokkeren.

Overkoepelend uitvoeringsschema van Kaspersky Threat Attribution Engine



Belangrijke product kenmerken

Biedt directe toegang tot een opslagplaats voor gecureerde gegevens van duizenden APT-actoren, exemplaren en grotere bedreigingen (via de anti-virus-engine)

Unieke inzichten in (meer dan 400) bekende campagnes die worden onderzocht door experts van Kaspersky

Biedt efficiënte geautomatiseerde of handmatige prioritering van dreigingen en schifting van meldingen

Er is de mogelijkheid om privé-actoren en -voorbeelden toe te voegen, zodat het product voorbeelden kan leren detecteren die lijken op bestanden in je privéverzameling

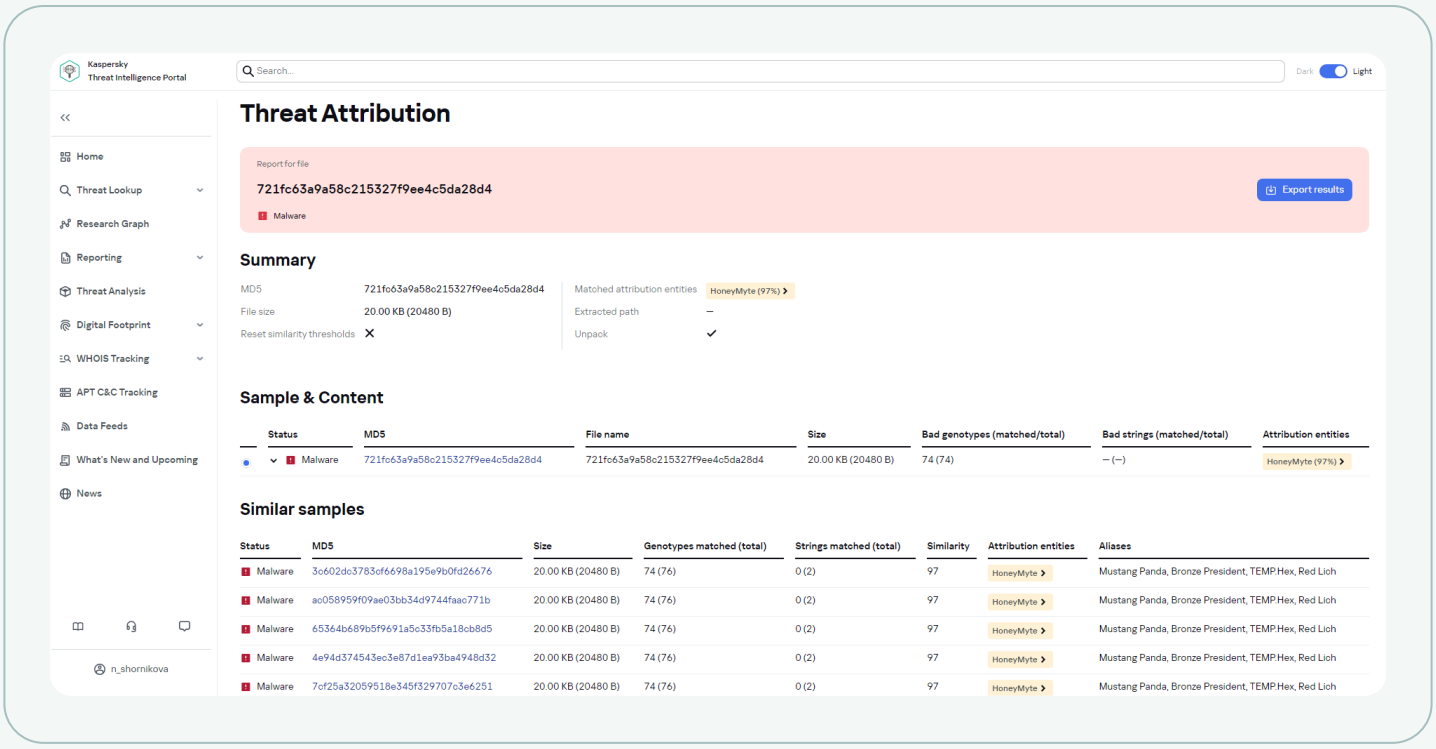
Handmatige upload van exemplaren en een geavanceerde REST API om te integreren met geautomatiseerde workflows

Ondersteunt de implementatie op cloud-infrastructuren zoals Amazon Web Services (AWS), waardoor je het product snel kunt instellen en kosten kunt besparen, aangezien je niet hoeft te investeren in hardware

Exporteren naar YARA-regels voor verder geautomatiseerd zoeken/scannen naar soortgelijke bestanden of integratie met oplossingen van externe partijen

Exporteren naar STIX 2.1-indeling (TXT- en JSON-indelingen worden ook ondersteund) voor verdere geautomatiseerde analyse van beveiligingslogs en integratie met oplossingen van externe partijen/ beveiligingscontroles

Mogelijkheid om wachtwoord-beveiligde archieven uit te pakken met aangepaste wachtwoorden



Eigen zoek methode

Om malware te koppelen aan attributie-entiteiten, wordt er bij Kaspersky Threat Attribution Engine gebruik gemaakt van een unieke eigen methode voor het zoeken naar soortgelijke genotypen en strings tussen bestanden. Deze methode omvat:

De genetica van een exemplaar analyseren

door de volgende onderdelen uit de code te extraheren:

- Genotypen - kenmerkende stukjes binaire code
- Strings - kenmerkende strings van tekens

De geanalyseerde bestanden automatisch doorzoeken

voor genotypen en strings die lijken op genotypen en strings van APT-exemplaren die in het verleden zijn geanalyseerd of al zijn gekoppeld aan attributie-entiteiten

Op basis van soortgelijke genotypen en strings

gevonden in APT-exemplaren, die een rapportage bieden over de herkomst van het geanalyseerde exemplaar, gerelateerde attributie-entiteiten en gelijkenissen tussen dit exemplaar en bekende APT-exemplaren

Kaspersky Threat Analysis

Kaspersky Similarity

Gelijkenis tussen bestanden

Om een effectieve verdedigingslinie op te bouwen, is het niet altijd noodzakelijk om te weten hoe je vijand eruitziet. Met Kaspersky Similarity kun je bestandsexemplaren identificeren met vergelijkbare functies om jezelf te beschermen tegen onbekende en ongrijpbare bedreigingen.

De cloudversie is beschikbaar via het Kaspersky Threat Intelligence Portal.

Vergelijkbaarheid

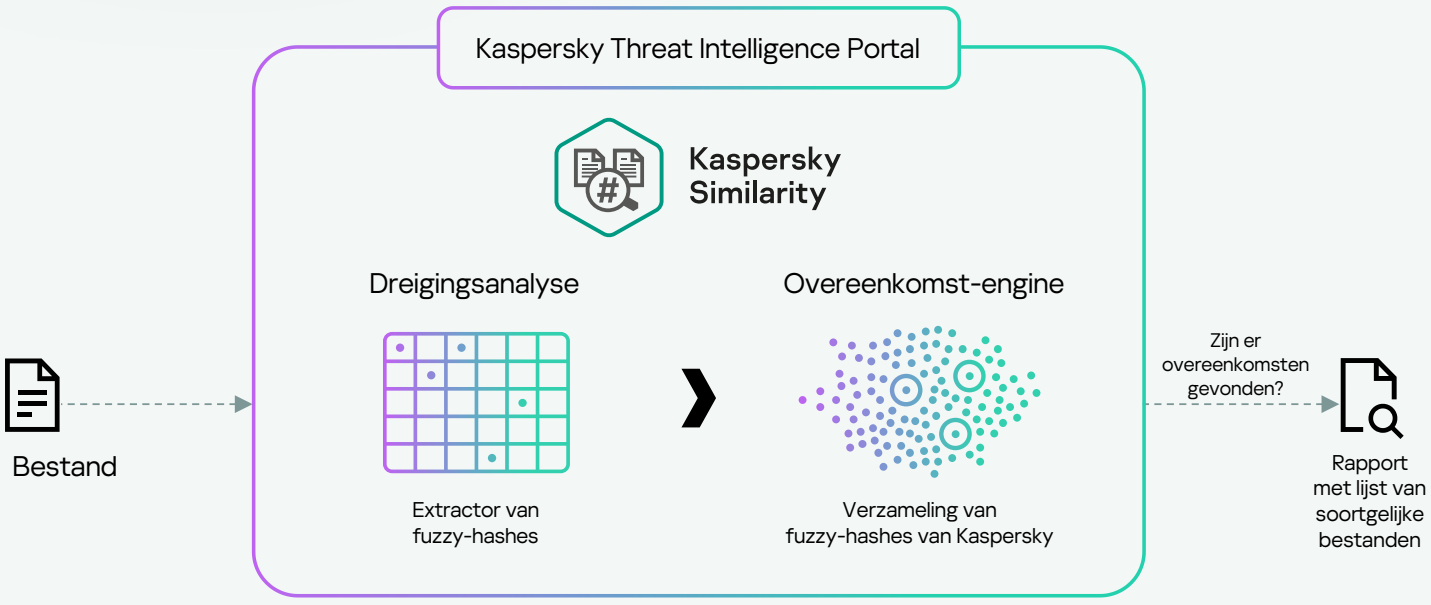
Kaspersky Similarity is een extra functie die beschikbaar is in het Threat Intelligence Portal voor gebruikers van zowel Kaspersky Research Sandbox als Kaspersky Threat Attribution Engine die helpt om bestanden te identificeren die op elkaar lijken en die soortgelijk gedrag vertonen.

Soortgelijke bestanden worden doorzocht en berekend voor het oorspronkelijke bestand door middel van een geavanceerde technologie die is bedacht door experts van Kaspersky en die gebruikmaakt van meer dan 50 unieke hash-typen. Dit zorgt voor precieze en zeer betrouwbare gelijkenisresultaten.

Waarom zou je dit moeten gebruiken?

Vind soortgelijke (en ongrijpbare) malware en zoek ernaar in je infrastructuur zodat je zeker weet dat je op de hoogte bent van kleine veranderingen in het exemplaar die zijn aangebracht door de aanvaller. Deze technologie is anders dan attributie: zelfs soortgelijke toegeschreven malware-bestanden kunnen worden opgespoord.

Overkoepelend werkschema van Kaspersky Similarity



Gelijkenis rapporten

Elk bestand heeft een specifieke indeling, gebruikte packers, secties, strings, belangrijke tabellen enz. De experts van Kaspersky hebben een reeks hashes ontwikkeld die de gelijkenis kunnen bepalen tussen verschillende bestanden op basis van deze kenmerken. Met Kaspersky Similarity kunnen gebruikers een verdacht bestand indienen, de fuzzy hashes extraheren en deze vergelijken met fuzzy hashes van bestanden die al in de bedreigingsdatabase van Kaspersky zitten. Als er overeenkomsten worden gevonden, wordt er een lijst gegenereerd met hashes van TOP soortgelijke schadelijke bestanden die al bekend zijn bij Kaspersky. Ze worden vervolgens gesorteerd op basis van het aantal gelijkenissen. Het rapport bevat extra context met metagegevens voor elk soortgelijk bestand:

- Mate van gelijkenis
- Status van bestand (malware, adware of anders)
- Naam van bedreiging
- Tijdstempels van de eerste en meest recente detectie
- Hoeveelheid hits (detecties)
- Bestands-hash
- Bestandstype
- Bestandsgrootte

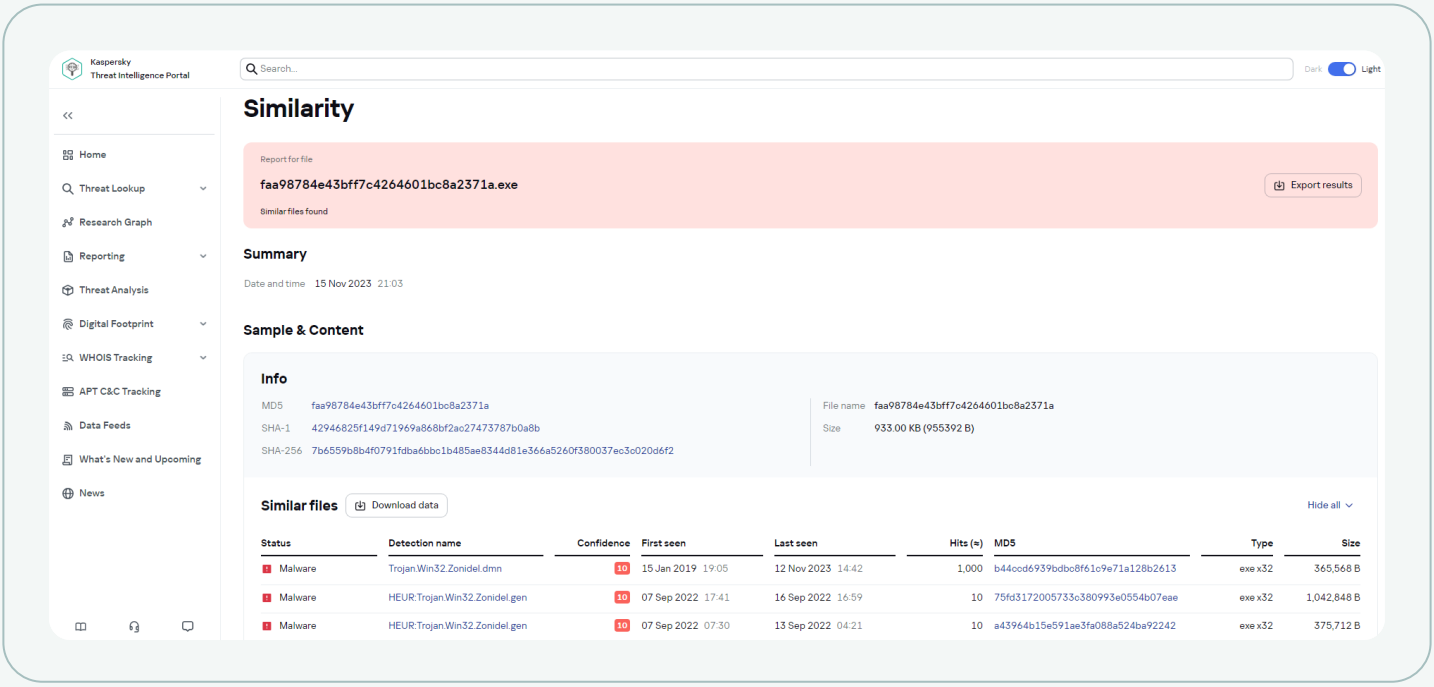
Belangrijke functies

Het maakt gebruik van een van de grootste databases in de industrie die bestaat uit schadelijke en schone bestanden die in de afgelopen 25 jaar zijn verzameld. Hierdoor krijg je de hoogste precisie bij het vergelijken van bestanden

Handmatige upload van exemplaren en een geavanceerde REST API om te integreren met geautomatiseerde workflows

Het wordt gratis aangeboden aan gebruikers van Kaspersky Research Sandbox en Kaspersky Threat Attribution om de effectiviteit te verhogen van beide technologieën en om uitgebreide informatie te geven over het geanalyseerde bestand

Het wordt al op grote schaal gebruikt door experts van Kaspersky om nieuwe bedreigingen te onderzoeken en nog betere bescherming tegen bedreigingen te bieden. Dit wordt regelmatig bewezen door onze topresultaten volgens onafhankelijke tests:



Gebruiksscenario's van Kaspersky Threat Analysis

Kaspersky Threat Analysis biedt weloverwogen instrumenten waarmee onbekende bedreigingen kunnen worden opgespoord en die veelvuldig kunnen worden gebruikt in de volgende scenario's:

Afhandeling van incidenten

Ongrijpbare dreigingen onthullen

Statische/dynamische analyse van verdachte bestanden

Het verband onthullen tussen een nieuwe soort malware en een bepaalde bedreigingsactor om eventuele nieuwe aanvallen te identificeren

Dreigingsopsporing

Scannen van de infrastructuur op IoC's die worden ontvangen via een rapport

Mogelijke schadelijke wijzigingen vinden in bekende schone bestanden

Gedeelde IoC's identificeren tussen onbekende en bekende schadelijke bestanden

Malwareanalyse

Analyse van onbekende bedreigingen

Vind gerelateerde malware om te helpen met omgekeerde engineering of verborgen bestanden

Kaspersky Threat Analysis is een flexibele onderzoekstool met onderling verbonden onderdelen. Hiermee kan een uitgebreide en meerlaagse beoordeling worden uitgevoerd voor verdachte objecten om zo geavanceerde aanvallen te kunnen identificeren en te classificeren. Het helpt SOC-teams, beveiligingsonderzoekers en malware-analisten om op de hoogte te blijven van bestaande en opkomende bedreigingen op het gebied van malware. Hierdoor kunnen ze snel kritieke bedreigingen prioriteren, aanpakken en ze op effectievere wijze herstellen.

Kaspersky Threat Analysis

Meer informatie

www.kaspersky.nl

#kaspersky
#bringonthefuture