kaspersky BRING ON THE FUTURE

Kaspersky Threat Attribution Engine

Het volgen, analyseren, interpreteren en inperken van voortdurend veranderende IT-beveiligingsdreigingen is een enorme onderneming. Dreigingsanalyse biedt veel toegevoegde waarde en is meer dan alleen een hype binnen de branche voor informatiebeveiliging. Dreigingstoewijzing is waarschijnlijk het belangrijkste element van dreigingsanalyse.

Hoofdkenmerken van het product:

- Directe toegang tot een bibliotheek met beheerde gegevens over honderden APT-actoren en -voorbeelden
- Efficiënte geautomatiseerde of handmatige prioritering van dreigingen en schifting van meldingen
- De mogelijkheid om privé-actoren en -voorbeelden toe te voegen, zodat het product voorbeelden kan leren detecteren die lijken op bestanden in uw privécollectie
- Handmatige uploads van voorbeelden en een open API voor integratie met geautomatiseerde workflows
- Kan worden geïmplementeerd in een beveiligde, geïsoleerde omgeving, om zo uw systemen en gegevens te beschermen en om aan alle nalevingsvereisten te voldoen
- Waarborgt op absolute wijze de privacy en vertrouwelijkheid van alles wat wordt ingediend en voorkomt dat gevoelige informatie bloot komt te liggen

Daar is een duidelijke reden voor. Vanwege de complexe processen voor onderzoek en reverse engineering zit er gemiddeld te veel tijd tussen de detectie van zeer geavanceerde dreigingen en de reactie erop. In veel gevallen kunnen aanvallers hun doelen bereiken binnen die periode. Correcte en tijdige toewijzing verkort de reactietijd bij incidenten van uren naar minuten. Bovendien wordt hiermee het aantal foutpositieve resultaten verlaagd.

Het kan echter jaren duren om een doelgerichte aanval te identificeren, een profiel van de aanvallers op te stellen en toewijzingsfactoren te maken voor de verschillende dreigingsactoren. Dit is een lang en grondig proces. Om een werkend toewijzingsmodel op te stellen, hebt u ook een enorme hoeveelheid gegevens nodig, verzameld gedurende meerdere jaren, plus een team van deskundige onderzoekers met de juiste ervaring. Samen volgen onderzoekers de activiteiten van verschillende groepen en vullen ze de database met de verzamelde stukjes informatie. Deze database wordt een waardevolle bron die als tool kan worden gedeeld.

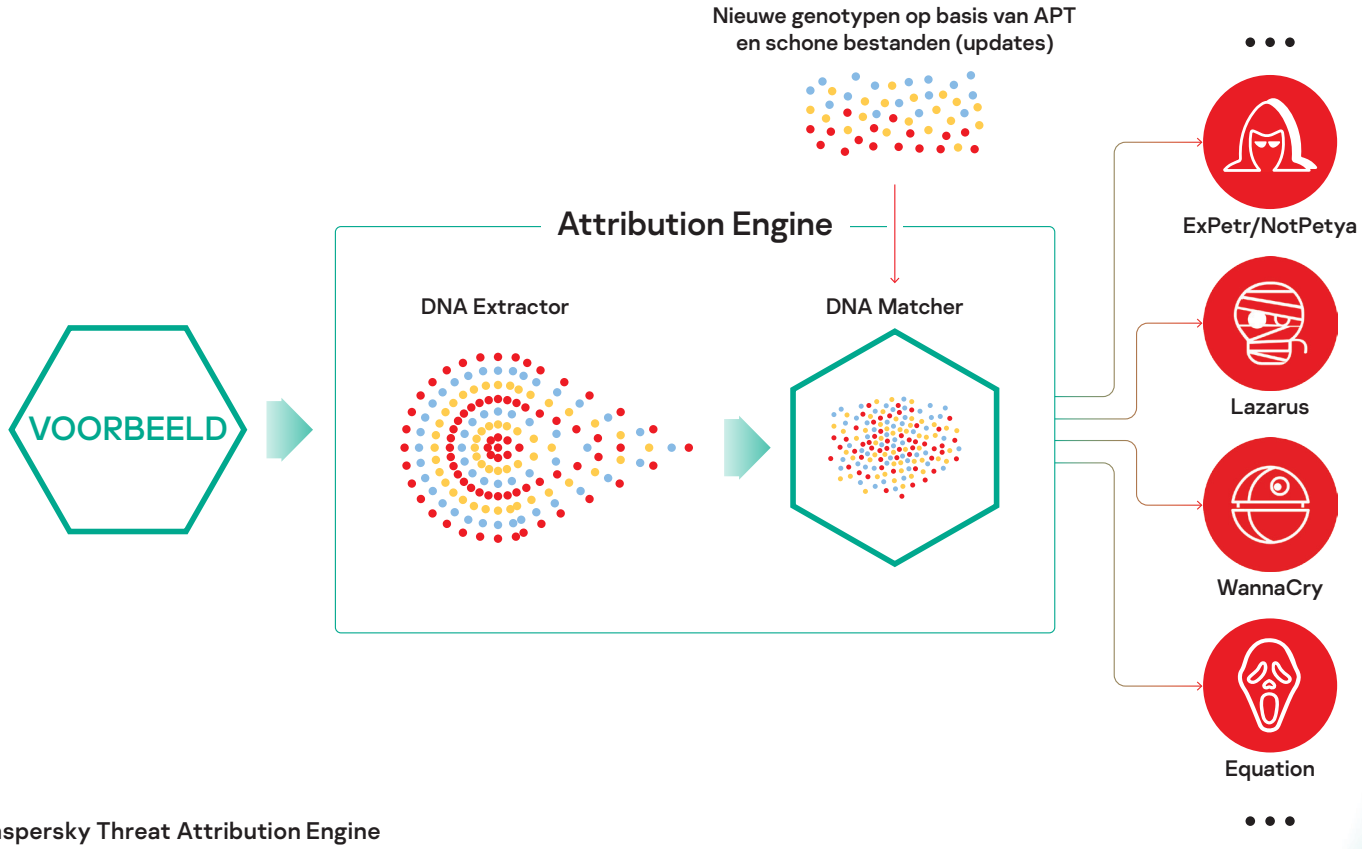
Kaspersky Threat Attribution Engine bevat een database met APT-malwarevoorbeelden en schone bestanden die gedurende de afgelopen 22 jaar door Kaspersky-experts zijn verzameld. We volgen meer dan 600 APT-dreigingsactoren en -campagnes, en we brengen elk jaar meer dan 120 APT-analyserapporten uit. Onze uitgebreide APT-verzameling met meer dan 60.000 bestanden is buitengewoon actueel dankzij ons continue onderzoek. Het verbetert de detectie van valse vlaggen en maakt de toewijzing zo nauwkeurig mogelijk middels geautomatiseerde tools.

Met het product kunnen voorbeelden op unieke wijze worden vergeleken, waarbij tegelijkertijd foutpositieve resultaten worden voorkomen. Het product kan een nieuwe aanval snel koppelen aan bestaande APT-malware, eerdere doelgerichte aanvallen en hackersgroepen. Het kan risicovolle dreigingen onderscheiden van minder serieuze incidenten en tijdig beschermende maatregelen treffen om te voorkomen dat een aanvaller toegang krijgt tot het systeem.

Hoe het werkt

Kaspersky Threat Attribution Engine analyseert de 'genetica' van malware door automatisch te zoeken naar code die lijkt op eerder onderzochte APT-voorbeelden en de bijbehorende dreigingsactoren. Het vergelijkt de 'genotypen', d.w.z. kleine binaire stukjes van de ontlede bestanden, met de database met APT-malwarevoorbeelden, en genereert een rapport over de malwareherkomst, dreigingsactoren en bestandsgelijkenis met de bekende APT-voorbeelden. Ook stelt het product beveiligingsteams in staat om privé-actoren en -objecten toe te voegen aan de database. Daarmee kan het product voorbeelden leren herkennen die lijken op bestanden in uw privécollectie. Met de Threat Attribution Engine duurt het toewijzingsproces nog maar enkele seconden – dus niet meer enkele jaren zoals vroeger.

Het product kan worden geïmplementeerd in een veilige, geïsoleerde omgeving. Derden hebben dus geen toegang tot de verwerkte informatie en ingediende objecten. Er is een API-interface om de Engine te koppelen aan andere tools en frameworks, zodat u toewijzing kunt implementeren in uw bestaande infrastructuur en geautomatiseerde processen.



Kaspersky Threat Attribution Engine

Gedetailleerde informatie over de gerelateerde APT-actor is beschikbaar in Kaspersky APT Intelligence-rapporten[1]. Als abonnee op Kaspersky APT Intelligence Reporting bieden we u unieke en onbeperkte toegang tot onze onderzoeken en ontdekkingen, met onder meer alle technische gegevens in verschillende indelingen voor elke APT zodra deze wordt ontdekt, inclusief alle dreigingen die nooit in de openbaarheid komen.

Kaspersky Threat Attribution Engine zorgt voor verdere uitbreiding en versterking van de Kaspersky-portfolio. De engine helpt nationale instanties voor cyberveiligheid en commerciële Security Operations Centers (SOC's) om een effectief proces voor incidentbeheer op te zetten.

Kaspersky Attribution Engine verbetert beveiligingsprocessen aanzienlijk door:

- Bestanden snel toe te wijzen aan bekende APT-actoren, om zo de motivaties, methoden en tools achter cyberincidenten bloot te leggen;
- Snel te evalueren of u het hoofddoelwit van een aanval bent of een bijkomend slachtoffer bent, om zo de juiste procedures voor inperking en respons op te zetten;
- Te zorgen voor effectieve en tijdige dreigingsinperking op basis van actiegerichte dreigingsinformatie over de APT-familie, aangeleverd in Kaspersky APT Intelligence Reporting.

1 Een abonnement op Kaspersky APT Intelligence Reporting moet afzonderlijk worden aangeschaft

Nieuws over cyberdreigingen: www.securelist.com
Nieuws over IT-beveiliging: business.kaspersky.com
IT-beveiliging voor het mkb: kaspersky.com/business
IT-beveiliging voor grote bedrijven: kaspersky.com/enterprise

www.kaspersky.com

Wij hebben ons bewezen. Wij zijn onafhankelijk. Wij zijn transparant. Wij zijn toegewijd aan het bouwen van een veiligere wereld, waarin technologie onze levens verbetert. Wij beveiligen deze technologie dus zodat iedereen overal toegang heeft tot de eindeloze mogelijkheden ervan. Wij bieden cyberveiligheid voor een veiligere toekomst.

Lees meer op kaspersky.com/transparency

Proven.
Transparent.
Independent.