kaspersky BRING ON THE FUTURE

Kaspersky Threat Attribution Engine

Å spore, analysere, tolke og begrense IT-sikkerhetstrusler i kontinuerlig utvikling er en enorm oppgave. Trusseletterretning har en reell verdi ut over å være et ganske opphausset satsingsområde innen informasjonssikkerhetsbransjen, og trusseltilskrivelse er sannsynligvis det mest fremtredende og også mest omstridte temaet når det gjelder trusseletterretning.

Hovedpunkter om produktet:

- gir øyeblikkelig tilgang til et repositorium av kuraterte data om hundrevis av APT-aktører og -eksempler
- muliggjør effektiv automatisert eller manuell trussel- og varselprioritering
- omfatter funksjonalitet for å legge til private aktører og eksempler og på denne måten lære produktet opp til å oppdage eksempler som ligner på filer i din private samling
- har en funksjon for manuell opplasting av eksempler og åpent API for integrasjon med automatiserte arbeidsflyter
- kan distribueres i sikre og fysisk separate miljøer for å beskytte systemene og dataene dine og oppfylle alle krav til samsvar
- sikrer personvern og konfidensialitet fullstendig ved all innsending, slik at sensitiv informasjon ikke eksponeres

Ikke uten grunn. Den gjennomsnittlige tiden fra oppdagelse av svært avanserte trusler til respons på disse er vanligvis for lang på grunn av komplekse undersøkelser og prosesser med omvendt utvikling. I mange tilfeller er det nok til at angriperne når målene sine. Riktig og rask tilskrivelse bidrar ikke bare til å forkorte responstiden for hendelser fra timer til minutter, men også til å redusere antallet falske positive resultater.

Det å identifisere et målrettet angrep, profilere angriperne og utarbeide tilskrivelsesfaktorer for de ulike trusselaktørene er en lang og omstendelig prosess som kan ta år å fullføre. En fungerende tilskrivelse forutsetter også en stor mengde data som er akkumulert over flere år, i tillegg til et høyt kvalifisert team av forskere med erfaring innen denne typen undersøkelser. Sammen følger forskerne med på aktiviteten til ulike grupper og fyller databasen med aktuell informasjon. Denne typen database blir en verdifull ressurs som kan deles som et verktøy.

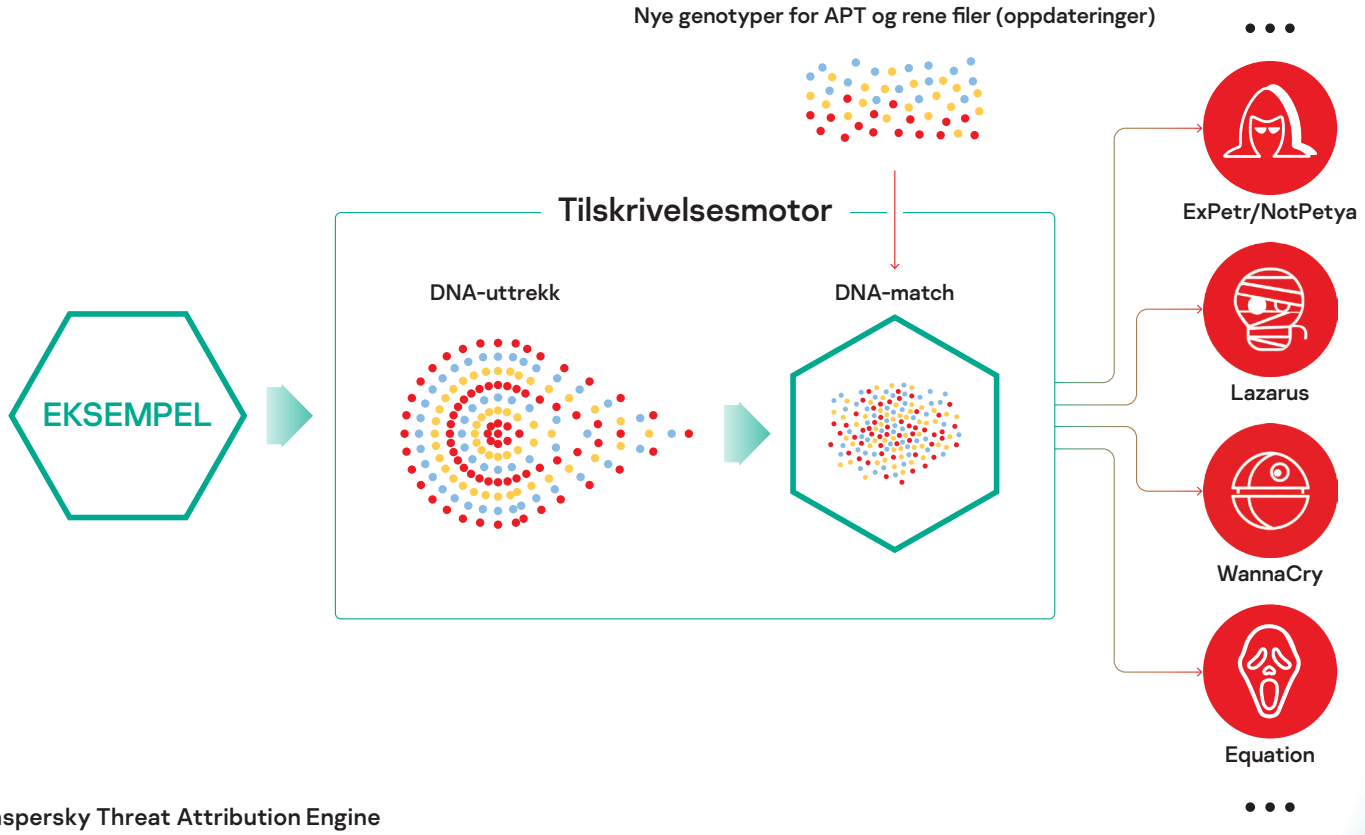
Kaspersky Threat Attribution Engine inneholder en database med eksempler på skadelig programvare (APT) som er samlet av Kaspersky-eksperter i over 22 år. Vi sporer over 600 APT-aktører og -kampanjer og utgir over 120 APT-etterretningsrapporter hvert år. Vår pågående forskning bidrar til å oppdatere den store APT-samlingen, som inneholder over 60 000 filer. Denne samlingen gir forbedret oppdagelse av falske flagg, slik at tilskrivelsen blir så nøyaktig som mulig ved bruk av de automatiserte verktøyene.

Produktet muliggjør en unik tilnærming til arbeidet med å sammenligne eksempler med tanke på likheter og samtidig sikre at antallet falske positive resultater reduseres til null. Det kan raskt koble et nytt angrep til kjent skadelig programvare (APT), tidligere målrettede angrep og hackergrupper, og dermed gjøre det enklere å se høyrisikotrusselen blant mindre alvorlige hendelser og iverksette beskyttende tiltak raskt for å forhindre at en angriper får innpass i systemet.

Hvordan det fungerer

Kaspersky Threat Attribution Engine analyserer «genene» til skadelig programvare for å se etter kodelikheter med tidligere undersøkte APT-eksempler og tilknyttede aktører på en automatisert måte. Løsningen sammenligner «genotypene», dvs. små binære biter av de dekomponerte filene, med databasen over skadelig programvare (APT) og leverer en rapport om opprinnelsen til skadelig programvare, trusselaktører og likheter med filer, med kjente APT-eksempler. Produktet gjør det dessuten mulig for sikkerhetsteam å legge til private aktører og objekter i databasen og lære produktet opp til å oppdage eksempler som ligner på filer i din private samling. Med Threat Attribution Engine tar tilskrivelsesprosessen sekunder i stedet for år, slik det var før.

Produktet kan distribueres i et sikkert og fysisk separat miljø, slik at uvedkommende ikke får tilgang til den behandlede informasjonen og innsendte objekter. Ved hjelp av API-grensesnittet kan motoren kobles til andre verktøy og rammeverk for å implementere tilskrivelse i eksisterende infrastruktur og automatiserte prosesser.



Kaspersky Threat Attribution Engine

Rapporter fra APT-etterretning fra Kaspersky inneholder detaljert informasjon om den aktuelle APT-aktøren[1]. Som abonnent på Kaspersky APT Intelligence Reporting får du unik, kontinuerlig tilgang til våre undersøkelser og funn, inkludert fullstendige tekniske data som leveres i en rekke formater, om hver APT idet den blir avslørt, inkludert alle de truslene som aldri vil bli offentlig kjent.

Kaspersky Threat Attribution Engine utvider og styrker Kasperskys portefølje ytterligere for nasjonale nettsikkerhetsorganer og kommersielle SOC-er (Security Operations Centers) ved å tilby disse hjelp til å etablere en effektiv prosess for håndtering av hendelser.

Kaspersky Attribution Engine gir en betydelig forbedring av sikkerhetsarbeidet ved å bidra til følgende:

- raskt tilskrive filer kjente APT-aktører for å avdekke motivasjonen, metodene og verktøyene bak netthendelser
- hurtig finne ut om du er hovedmålet for angrepet eller ikke, for å få på plass egnede prosedyrer for begrensning og respons
- sikre rask og effektiv trusselbekjempelse i samsvar med handlingsrettet trusseletterretning om APT-familien levert av Kaspersky APT Intelligence Reporting

1 Et abonnement på Kaspersky APT Intelligence Reporting må kjøpes separat

Nyheter om nettrusler: www.securelist.com
Nyheter om IT-sikkerhet: business.kaspersky.com
IT-sikkerhet for SMB: kaspersky.com/business
IT-sikkerhet for større bedrifter: kaspersky.com/enterprise

www.kaspersky.com

Vi er anerkjente. Vi er uavhengige. Vi er tydelige. Vi er opptatt av å bygge en tryggere verden, der teknologi gjør livene våre bedre. Derfor sikrer vi den, slik at alle overalt får de endeløse mulighetene den gir. Nettsikkerhet for en tryggere fremtid.

Finn ut mer på kaspersky.com/transparency

Proven.
Transparent.
Independent.