kaspersky BRING ON THE FUTURE

Kaspersky Threat Attribution Engine

Sporing, analyse, fortolkning og afhjælpning af konstant skiftende IT-sikkerhedstrusler er en stor forpligtelse. Trusselindsigt har en værdi, som går videre end den nuværende hype vedrørende en ny tendens i informationssikkerhedsbranchen, og trusselsidentifikation er sandsynligvis det mest fremtrædende interesse- og stridspunkt, når det drejer sig om trusselindsigt.

Produkthøjdepunkter:

- Giver øjeblikkelig adgang til et lager med organiserede data om hundreder af APT-aktører og -eksempler
- Giver mulighed for effektiv automatiseret eller manuel prioritering af trusler og test af advarsler
- Funktionalitet til tilføjelse af private aktører og eksempler, så produktet kan oplæres til at registrere eksempler, som ligner filer i din private samling
- Manuel opload af eksempler og åben API til integration med automatiske arbejdsprocesser
- Kan implementeres i sikre, air-gap-miljøer for at beskytte dine systemer og data samt opfylde alle krav ift. overholdelse
- Opretholder effektiv beskyttelse af personlige oplysninger og fortrolighed for alle indsendelser for at undgå at afsløre følsomme oplysninger

Og der er en logisk årsag til dette. Den gennemsnitlige tid fra registrering til reaktion på yderst sofistikerede trusler er normalt for lang pga. kompleks undersøgelse og reverse engineering-processer. I mange tilfælde er det nok til, at hackere kan nå deres mål. Korrekt og rettidig kildeidentifikation medvirker til ikke blot at forkorte responstiden for hændelser fra timer til minutter, men reducerer også antallet af falske positiver.

Det er et langvarigt og krævende job at identificere et målrettet angreb, identificere angriberne og oprette identifikationsfaktorer for de forskellige trusselsaktører, det kan tage flere år. Oprettelse af fungerende kildeidentifikation kræver også store mængder akkumulerede data samt højtkvalificerede researchere, som har erfaring med efterforskning. Researchere følger normalt forskellige gruppers aktiviteter og indlæser oplysninger i databasen. Og databasen bliver en værdifuld ressource, der kan deles som et værktøj.

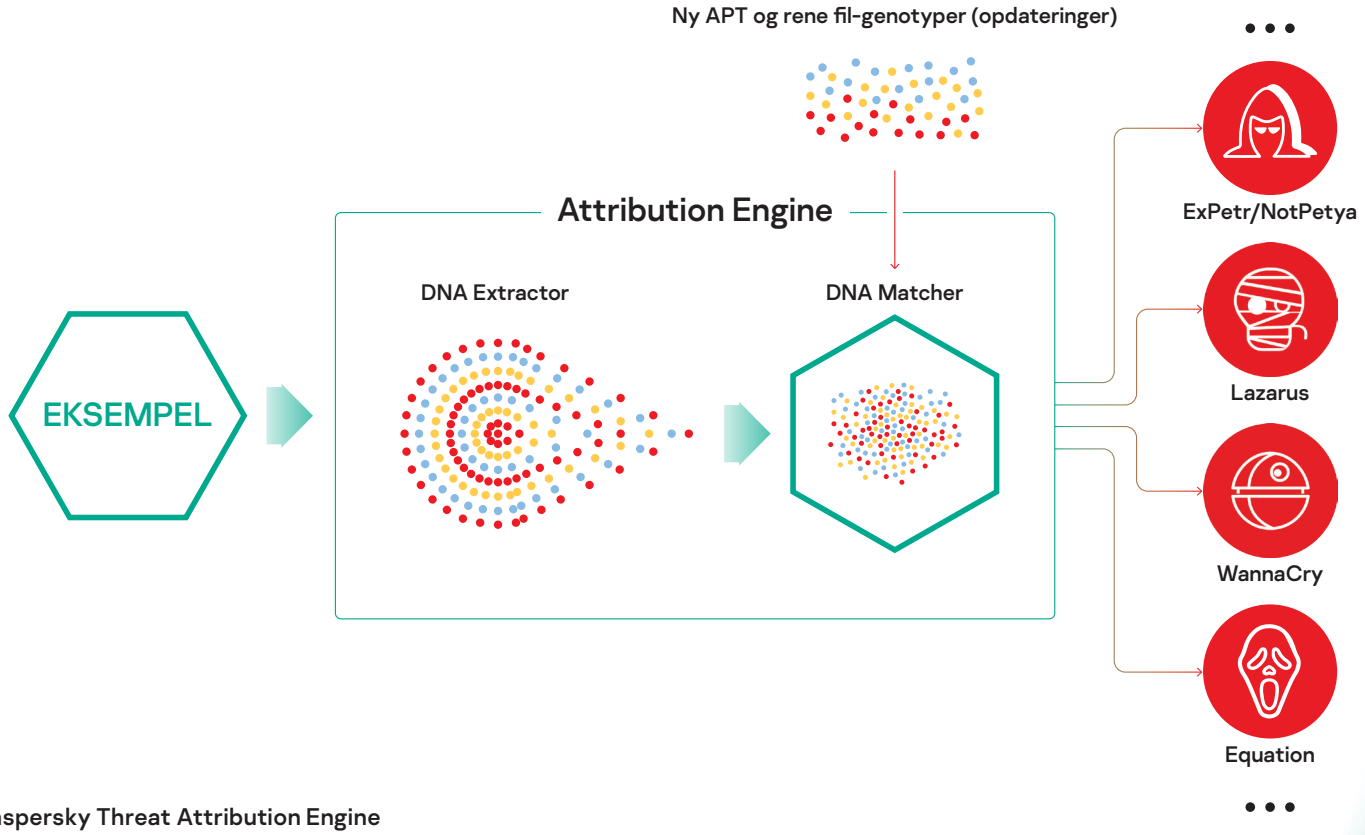
Kaspersky Threat Attribution Engine indeholder en database med APT-malwareprogrammer og rene filer, som Kasperskys eksperter har indsamlet over 22 år. Vi følger 600+ trusselsaktører og -kampagner med 120+ APT Intelligence-rapporter, som udgives hvert år. Vores løbende research understøtter aktualiteten af den omfattende APT-samling, som indeholder 60K+ filer. Den forbedrer registrering af falske flag og gør kildeidentifikation så nøjagtig som muligt ved hjælp af de automatiserede værktøjer.

Produktet gør det muligt at sammenligne eksempler vedrørende ligheder, samtidig med at der ikke opstår falske positiver. Det kan hurtigt linke et nyt angreb til kendt APT-malware og hjælper med at se højrisikotruslen blandt mindre alvorlige hændelser og træffe rettidige beskyttelsesforanstaltninger for at forhindre en hacker i at få fodfæste i systemet.

Sådan fungerer det

Kaspersky Threat Attribution Engine analyserer "genetikken" i malware og kigger efter kodeligheder i tidligereundersøgte APT-eksempler og linkede aktører på en automatiseret måde. Det sammenligner "genotyperne", dvs. små binære dele af de nedbrudte filer, med APT-malware-eksemplerne i databasen og udarbejder en rapport om malwarens oprindelse, trusselsaktører og fillighed med kendte APT-eksempler. Derudover giver produktet sikkerhedsmedarbejdere mulighed for at tilføje private aktører og emner i deres database og oplære produktet til at registrere eksempler, som ligner filer i din private samling. Med Threat Attribution Engine tager kildeidentifikationsprocessen kun sekunder i forhold til de flere år, det tidligere tog.

Produktet kan implementeres i et sikkert, "air-gap"-miljø, som forhindrer tredjeparter i at få adgang til de behandlede oplysninger og indsendte emner. Der findes en API-grænseflade, som kan forbinde programmet til andre værktøjer og strukturer for at implementere kildeidentifikation i eksisterende infrastrukturer og automatiserede processer.



Kaspersky Threat Attribution Engine

Detaljerede oplysninger om den relaterede APT-aktør findes i Kaspersky APT Intelligence-rapporter[1]. Som abonnent på Kaspersky APT Intelligence Reporting giver vi dig løbende adgang til vores undersøgelser og opdagelser, herunder fyldestgørende tekniske data i en lang række formater, der afdækkes på hver APT, idet de afdækkes – herunder alle de trusler, der aldrig vil blive offentliggjort.

Kaspersky Threat Attribution Engine udvider og styrker yderligere Kasperskys portefølje for nationale cybersikkerhedsinstitutioner og kommercielle SOC'er (Security Operations Centers) ved at bistå dem med at etablere en effektiv hændelsesstyringsproces.

Kaspersky Attribution Engine forbedrer i høj grad sikkerhedsoperationer og bidrager med:

- Hurtigt at knytte filer til kendte APT-aktører for at afsløre motivation, metoder og værktøjer bag cyberhændelser
- Hurtigt at evaluere, om du er mål for et angreb eller et utilsigtet offer for at konfigurere korrekt isolation og procedurer for respons
- At sikre effektiv og rettidig minimering af trusler i henhold til trusselindsigt, der kan handles på, i den APT-serie, der findes i Kaspersky APT Intelligence Reporting

1 Et abonnement på Kaspersky APT Intelligence Reporting skal købes separat

Nyheder om IT-sikkerhedstrusler: www.securelist.com
Nyheder om IT-sikkerhed: business.kaspersky.com
IT-sikkerhed for små og mellemstore virksomheder: kaspersky.com/business
IT-sikkerhed for større virksomheder: kaspersky.com/enterprise

www.kaspersky.com

Vi er anerkendte. Vi er uafhængige. Vi er transparente. Vi har forpligtet os til at opbygge en mere sikker verden, hvor teknologi kan gøre vores liv bedre. Det er derfor, at vi gør den sikker, så alle kan få glæde af de uendelig muligheder, den bringer. Cybersikkerhed for en mere sikker fremtid.

Få mere at vide på kaspersky.com/transparency

Proven.
Transparent.
Independent.