kaspersky BRING ON THE FUTURE

Kaspersky Threat Attribution Engine

Att övervaka, analysera och avvärja högdynamiska hot mot IT-säkerheten kräver ansenliga insatser. Hotinformation är viktig även utanför en liten grupp inom säkerhetsindustrin, och hotattribution är förmodligen det som är föremål för störst intresse och diskussion när det gäller hotinformation.

Viktiga punkter:

- Ger omedelbar åtkomst till ett lager med bearbetade data om hundratals APT-aktörer och exempel
- Möjliggör effektiv prioritering av hot och varningar, manuellt eller automatiskt
- Möjlighet för säkerhetsteam att lägga till privata aktörer och exempel och träna produkten att identifiera prov som liknar filer i den privata samlingen
- Manuell exempeluppladdning och öppet API för integrering med automatiska arbetsflöden
- Kan driftsättas i säkra avgränsade miljöer för att skydda dina system och data och uppfylla alla efterlevnadskrav
- Kan driftsättas i säkra miljöer med luftgap för att skydda dina system och data och uppfylla alla efterlevnadskrav

Det finns en tydlig orsak till det. Den genomsnittliga tiden från upptäckt till svar på mycket avancerade hot är vanligtvis för lång på grund av komplexa utredningar och processer för att få tillgång till programkoden. I många fall räcker detta för att angriparna ska kunna nå sina mål. Rätt attribution i rätt tid bidrar inte bara till att korta tiderna för incidentreaktion från timmar till minuter utan även till att minska antalet falskt positiva identifieringar.

Att identifiera en målriktad attack, profilera angriparna och skapa attributionsfaktorer för de olika angreppsaktörerna är ett långt och krävande arbete som kan ta flera år. För att ta fram fungerande attribution krävs också en stor mängd ackumulerade data från flera år och ett skickligt forskarteam med erfarenhet av undersökningar. Vanligtvis följer forskarna aktiviteten hos olika grupper och fyller på databasen med denna information. Databasen blir en värdefull resurs som kan delas som ett verktyg.

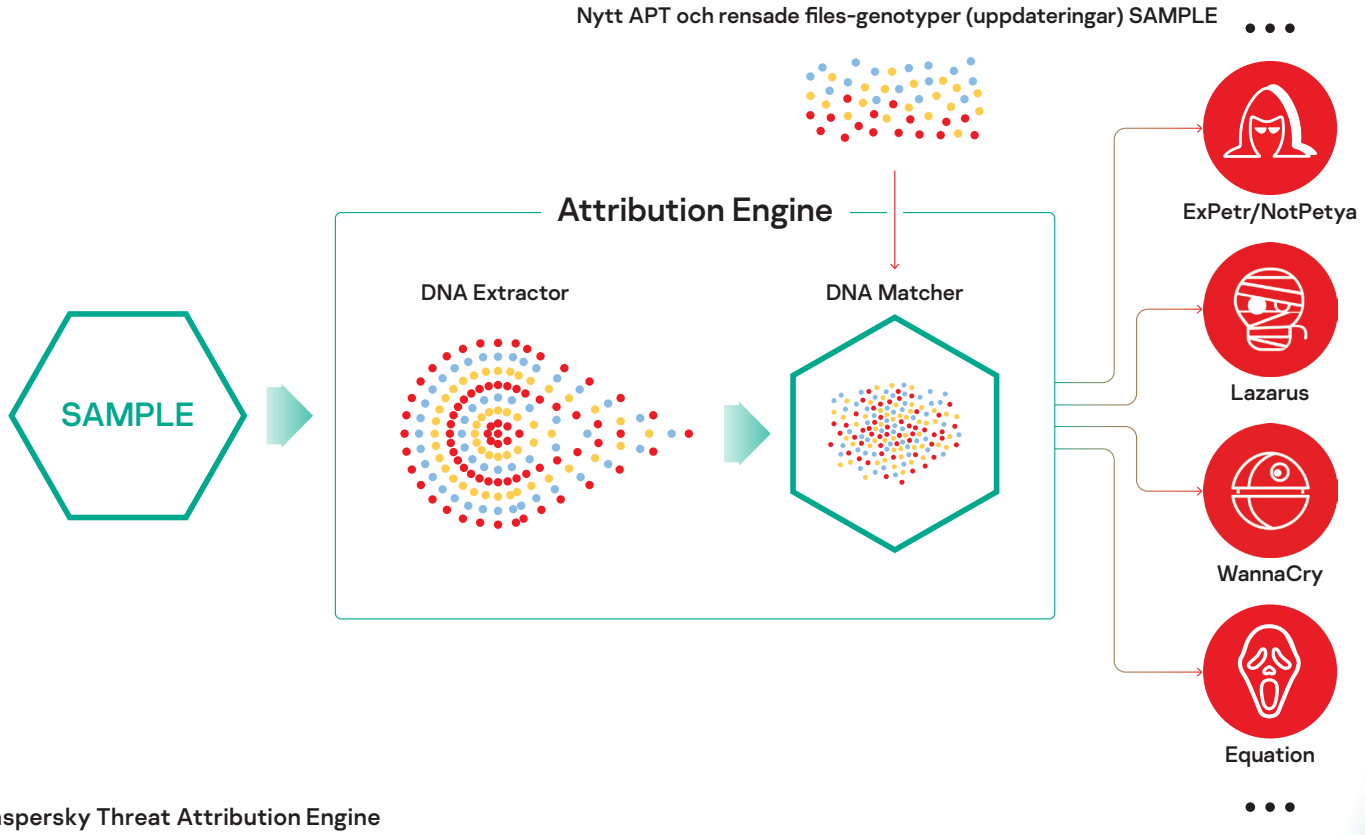
Kaspersky Threat Attribution Engine innehåller en databas med prov på skadliga APT-program och -filer som har samlats in av Kaspersky-experter under 22 år. Vi spårar mer än 600 APT-aktörer och publicerar mer än 120 APT-informationsrapporter varje år. Vår pågående forskning stödjer uppdateringen av den stora APT-samlingen som omfattar över 60 000 filer. Den förbättrar identifieringen av falsk flaggning och gör attributionen så exakt som möjligt med hjälp av de automatiska verktygen.

Produkten möjliggör en unik metod för jämförelse av exempel för att hitta likheter samtidigt som man får noll falska identifieringar. Den kan snabbt länka en ny attack till kända skadliga APT-program, tidigare målriktade attacker och hackargrupper, vilket hjälper till att identifiera högriskhot och skilja dem från mindre allvarliga incidenter, och också snabbt vidta skyddsåtgärder för att förhindra att angriparen får fäste i systemet.

Så här fungerar det

Kaspersky Threat Attribution Engine analyserar "genetiken" i skadliga program och letar efter kodelement som liknar tidigare undersökta APT-exempel och länkade aktörer på ett automatiserat sätt. Det jämför "genotyperna", d.v.s. små binära delar av de nedbrutna filerna, med APT-databasen med exempel på skadlig kod och ger en rapport om den skadliga kodens ursprung, hotaktörer och likheter i filerna med kända APT-exempel. Produkten låter också säkerhetsteam lägga till privata aktörer och objekt i databasen och träna produkten att identifiera exempel som liknar filerna i den privata samlingen. Med Threat Attribution Engine tar attributionsprocessen bara några sekunder, att jämföra med flera år som tidigare.

Produkten kan distribueras i en säker miljö med luftgap, som förhindrar att någon tredje part får åtkomst till den bearbetade informationen och inskickade objekt. Det finns ett API-gränssnitt för att ansluta Engine till andra verktyg och ramverk för att implementera attribution i befintliga infrastrukturer och automatiska processer.



Kaspersky Threat Attribution Engine

Mer information om den relaterade APT-aktören finns i Kasperskys APT-analysrapporter[1]. Som prenumerant på Kasperskys APT-analysrapporter får du unika, löpande analyser. Vi levererar bland annat kompletta tekniska data i en rad olika format om olika APT:er direkt när vi identifierar dem. Det gäller även hot som allmänheten aldrig får kännedom om.

Kaspersky Threat Attribution Engine utökar och stärker Kasperskys portfölj för nationella cybersäkerhetsmyndigheter och kommersiella säkerhetscenter (SOC, Security Operations Center) genom att hjälpa dem upprätta en effektiv process för incidenthantering.

Kaspersky Attribution Engine förbättrar säkerhetsarbetet märkbart genom att bidra till följande:

- Snabb attribution av filer till kända APT-aktörer för att avslöja motivation, metoder och verktyg bakom cyberincidenterna
- Snabb bedömning av om du är attackens huvudsakliga mål eller ett sidomål för att skapa lämpliga isolerings- och åtgärdsprocesser
- Effektiv och snabb minskning av hot i enlighet med åtgärdbar hotanalys på APT-familjen i Kasperskys APT-analysrapporter

1 En prenumeration på Kaspersky APT Intelligence Rapportering köps separat

Nyheter om cyberhot: www.securelist.com
IT-säkerhetsnyheter: business.kaspersky.com
IT-säkerhet för SMB: kaspersky.com/business
IT-säkerhet för stora företag: kaspersky.com/enterprise

www.kaspersky.com

Vi är beprövade. Vi är oberoende. Vi är transparenta. Vårt mål är att skapa en säkrare värld, där tekniken förbättrar våra liv. Det är därför vi gör den säkrare, så att alla kan dra nytta av de oändliga möjligheterna. Använd cybersäkerhet för en säkrare framtid.

Läs mer på kaspersky.com/transparency

Proven.
Transparent.
Independent.